

水道情報活用システム

基本仕様書 別冊

IoT ゲートウェイ外部仕様書 (改定案)

2019 年 12 月 26 日

水道施設情報整備促進事業委員会

- 目次 -

1. はじめに.....	1
1.1 本ドキュメントの目的.....	1
1.2 水道情報活用システム標準仕様のドキュメント.....	2
1.2.1 ドキュメント体系.....	2
1.2.2 対象読者と役割.....	3
1.2.3 本ドキュメントの対象読者.....	4
1.3 参考文献.....	5
1.4 用語の説明.....	8
1.5 本ドキュメントの記載範囲.....	10
1.6 本ドキュメントに記載する外部仕様の位置づけ.....	10
2. 概要.....	11
2.1 IoT ゲートウェイの役割と特徴.....	11
2.2 IoT ゲートウェイの機能における競争領域と協調領域.....	13
3. 機器ベンダー向け標準インターフェイス(デバイス)モジュール.....	15
3.1 機能概要.....	15
3.2 機能一覧.....	15
3.3 機能要件.....	16
3.3.1 IoT ゲートウェイ接続.....	16
3.3.2 IoT ゲートウェイ切断.....	17
3.3.3 定周期監視-定周期監視開始.....	17
3.3.4 定周期監視-定周期監視データ送信.....	18
3.3.5 定周期監視-定周期監視停止.....	20
3.3.6 即時取得.....	21
3.3.7 機器制御.....	22
3.3.8 公開鍵証明書ファイル取得.....	23
4. データセキュリティモジュール.....	25
4.1 機能概要.....	25
4.1.1 機能一覧.....	25

4.1.2 データ暗号化/データ復号方式	26
4.1.3 電子署名方式	36
4.1.4 データマスキング方式	42
4.2 機能要件.....	43
4.2.1 データ保護用証明書/秘密鍵取得機能	43
4.2.2 データ暗号化機能	44
4.2.3 データ復号機能	45
4.2.4 電子署名付与機能	46
4.2.5 電子署名検証機能	47
4.2.6 データマスキング機能	48
5. 一次データ蓄積モジュール.....	50
5.1 機能概要.....	50
5.2 機能一覧.....	50
5.3 機能要件.....	51
5.3.1 データ蓄積/提供-データ蓄積	51
5.3.2 データ蓄積/提供-データ提供	51
5.3.3 データ退避	52
6. デバイス接続モジュール.....	54
6.1 機能概要.....	54
6.2 機能一覧.....	54
6.3 機能要件.....	55
6.3.1 定周期監視-定周期監視開始	55
6.3.2 定周期監視-定周期監視データ受信	56
6.3.3 定周期監視-定周期監視停止	57
6.3.4 即時取得	57
6.3.5 機器制御	59
7. システム監視モジュール.....	61
7.1 機能概要.....	61

1. はじめに

1.1 本ドキュメントの目的

本ドキュメントは、社会インフラ水道情報活用システム(以下、水道情報活用システム)標準仕様における基本仕様の別冊である。

基本仕様書では、水道情報活用システムを実現する基本仕様として、水道情報活用システムの全体構成と基本的に守るべきルール、標準インターフェイスを規定している。

本ドキュメントは、基本仕様書で規定した水道情報活用システムの1つである、IoT ゲートウェイ仕様の詳細を記載したドキュメントである。

本ドキュメントは、IoT ゲートウェイ・デバイスベンダーが、IoT ゲートウェイに要求される仕様を把握した上で、どのような要件を実現した IoT ゲートウェイを構築・運用すればよいかを理解することを目的とする。

1.2 水道情報活用システム標準仕様のドキュメント

1.2.1 ドキュメント体系

水道情報活用システム標準仕様のドキュメント体系図を以下に示す(図 1-1)。

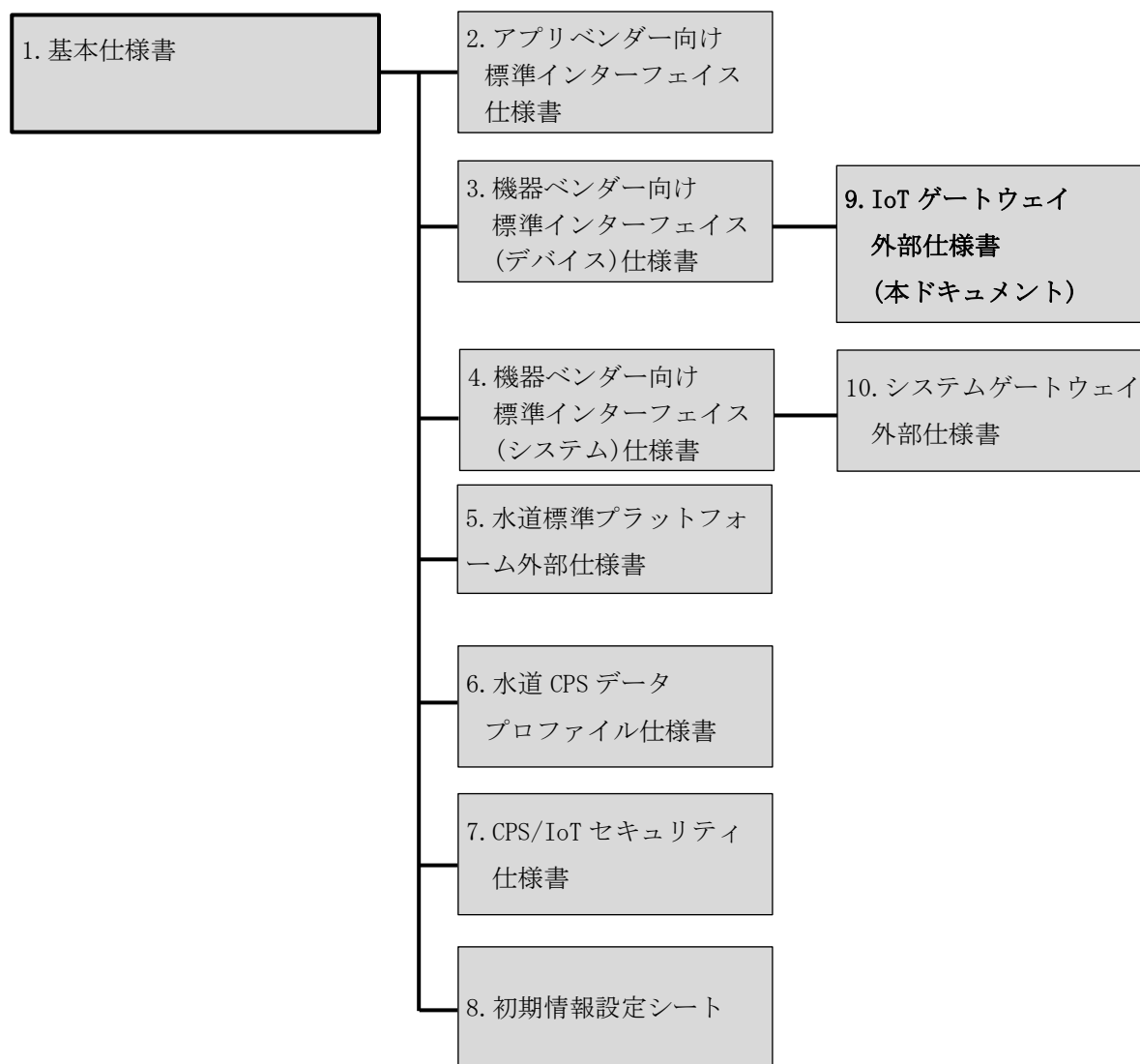


図 1-1: ドキュメント体系図

1.2.2 対象読者と役割

水道情報活用システム標準仕様の対象読者と役割を以下に示す。

① 事業体：

水道情報活用システム上のアプリケーションを利用して、デバイス・システムのデータを活用したサービスを享受する事業体。

② アプリケーション開発ベンダー：

水道情報活用システム上のアプリケーションを開発し、デバイス・システムのデータを活用したサービスを事業体に提供するベンダー。

③ IoT ゲートウェイ・デバイスベンダー：

水道情報活用システム上の IoT ゲートウェイを開発し、デバイスのデータを水道標準プラットフォームへ流通するベンダー。

④ システムゲートウェイ・システムベンダー：

水道情報活用システム上のシステムゲートウェイを開発し、各種台帳システムや料金システム等の業務システムのデータを水道標準プラットフォームへ流通するベンダー。

⑤ プラットフォーマー：

水道情報活用システム上の水道標準プラットフォームを提供し、デバイス・システムのデータを流通するサービス提供および運営を行う第三者機関。

⑥ システムインテグレーター：

水道情報活用システム全体の設計を行い、アプリケーション開発ベンダーや IoT ゲートウェイ・デバイスベンダー、システムゲートウェイ・システムベンダーを統率し、水道情報活用システムを事業体に導入するベンダー。

1.2.3 本ドキュメントの対象読者

本ドキュメントの対象読者を以下に示す(表 1-1)。

IoT ゲートウェイ外部仕様書(本ドキュメント)は、主に③IoT ゲートウェイ・デバイスベンダー、⑥システムインテグレーターが参照すべきドキュメントである。

表 1-1: 参照すべきドキュメントと対象読者

No	ドキュメント名		対象読者 (1.2.2 項を参照)					
			①	②	③	④	⑤	⑥
1	基本仕様書 (本ドキュメント)		○	○	○	○	○	○
2	別冊	アプリベンダー向け 標準インターフェイス仕様書	—	○	—	—	○	○
3		機器ベンダー向け 標準インターフェイス(デバイス)仕様書	—	—	○	—	○	○
4		機器ベンダー向け 標準インターフェイス(システム)仕様書	—	—	—	○	○	○
5		水道標準プラットフォーム外部仕様書	—	△	△	△	○	△
6		水道 CPS データプロファイル仕様書	—	○	○	—	○	○
7		CPS/IoT セキュリティ仕様書	—	○	○	○	○	○
8		初期情報設定シート	○	○	○	○	○	○
9		IoT ゲートウェイ外部仕様書	—	—	○	—	—	○
10		システムゲートウェイ外部仕様書	—	—	—	○	—	○

【凡例】 ○：必須、△：任意

1.3 参考文献

水道情報活用システム標準仕様を参照する際の参考文献を以下に示す(表 1-2)。

表 1-2: 参考文献

No	参考文献	説明
1	ISO 8601	日付と時刻の表記について規定する ISO による国際規格。 URL※： https://www.iso.org/iso-8601-date-and-time-format.html
2	MQTT Protocol Specification	水道標準プラットフォームで利用するメッセージングプロトコルである MQTT について、OASIS により規定されたプロトコル仕様。 URL※： http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html
3	OpenID Connect	認証プロトコルについて規定する、OpenID ファウンデーションによるプロトコル仕様。 URL※： http://www.openid.or.jp/document/
4	OpenID Connect Core 1.0	水道標準プラットフォームで利用するアイデンティティ連携プロトコル仕様。 URL※： http://openid.net/specs/openid-connect-core-1_0.html
5	RFC 2616	Hypertext Transfer Protocol (HTTP/1.1) について規定する IETF による技術仕様。 URL※： https://tools.ietf.org/html/rfc2616
6	RFC 2818	暗号化通信プロトコルである HTTP over TLS(本ドキュメントでは「HTTP(S)」と表記)について規定する、IETF によるプロトコル仕様。 URL※： https://tools.ietf.org/html/rfc2818

No	参考文献	説明
7	RFC 5246	セキュアな通信を行うためのプロトコルである Transport Layer Security(TLS)について規定する、IETF によるプロトコル仕様。 URL※ : https://tools.ietf.org/html/rfc5246
8	RFC 6455	水道標準プラットフォームで利用する通信プロトコルである WebSocket について、IETF により公開されたプロトコル仕様。 URL※ : https://tools.ietf.org/html/rfc6455
9	RFC 6750	OpenID Connect のベースである OAuth 2.0 のトークン仕様について規定する、IETF による技術仕様。 URL※ : https://tools.ietf.org/html/rfc6750
10	RFC 7231	HTTP/1.1 におけるセマンティクスとコンテンツについて規定する IETF による技術仕様。 URL※ : https://tools.ietf.org/html/rfc7231
11	XML Encryption Syntax and Processing	XML 暗号について規定する W3C 勧告。 URL※ : http://www.w3.org/TR/xmlenc-core1/
12	XML Signature Syntax and Processing	XML 署名について規定する W3C 勧告。 URL※ : http://www.w3.org/TR/xmlsig-core2/

※: 2017 年 7 月時点の URL を参考に記載

その他、参考にする報告書を以下に示す。

経済産業省「平成28年度 I o T 推進のための社会システム推進事業(スマート工場実証事業) 報告書」

http://www.meti.go.jp/policy/mono_info_service/mono/smart_mono/H28SmartFactory_DataProfile_Security_Report.pdf

http://www.meti.go.jp/policy/mono_info_service/mono/smart_mono/H28SmartFactory_DataProfile_Security_Report_Attachment1.pdf

http://www.meti.go.jp/policy/mono_info_service/mono/smart_mono/H28SmartFactory_DataProfile_Security_Report_Attachment2.pdf

経済産業省「平成28年度 I o T 推進のための社会システム推進事業(社会インフラ分野での I o T 活用のための基盤整備実証プロジェクト)」

http://www.meti.go.jp/meti_lib/report/H28FY/000060.pdf

http://www.meti.go.jp/meti_lib/report/H28FY/000061.pdf

http://www.meti.go.jp/meti_lib/report/H28FY/000062.pdf

1.4 用語の説明

水道情報活用システム標準仕様で使用する用語の説明を以下に示す(表 1-3)。

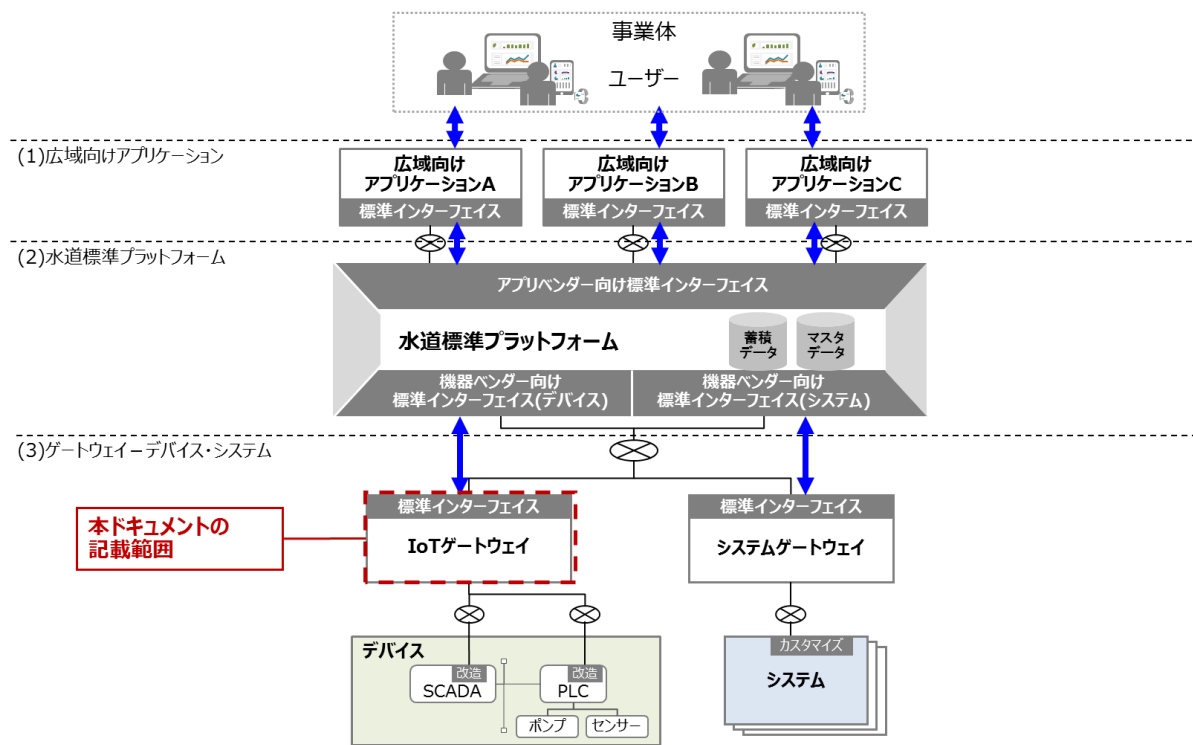
表 1-3: 用語の説明

No	用語	説明
1	AI (<u>A</u> rtificial <u>I</u> ntelligence)	コンピュータを使って学習・推論・判断等、人間の知能の働きを人工的に実現するもの。
2	API (<u>A</u> pplication <u>P</u> rogramming <u>I</u> nterface)	ソフトウェアコンポーネントが互いにやり取りするのに使用するインターフェイスの仕様。
3	水道情報活用システム	CPS/IoT を活用して、デバイス・システムのデータを流通させ、データを活用した付加価値の高いサービスを提供するシステム。
4	DUNS Number (<u>D</u> ata <u>U</u> niversal <u>N</u> umbering <u>S</u> ystem Number)	ダンアンドブラッドストリート(D&B)社が開発した9桁の企業識別コードのことで、世界の企業を一意に識別できる企業コード。
5	FQDN (<u>F</u> ully <u>Q</u> ualified <u>D</u> omain <u>N</u> ame)	完全修飾ドメイン名。ホスト名とドメイン名などすべてを省略せずに指定した文字列。
6	IANA (<u>I</u> nternet <u>A</u> ssigned <u>N</u> umbers <u>A</u> uthority)	IP アドレス・ドメイン名・ポート番号等の標準化・割り当て等インターネットに関連する番号を管理する組織。
7	JAN コード (<u>J</u> apanese <u>A</u> rticle <u>N</u> umber)	国際的な流通標準化機関である GS1 が定める国際標準の識別コードを設定するために必要となるコード。国際的には GS1 Company Prefix と呼ばれ、日本では最初の2桁が「45」又は「49」で始まる9桁又は7桁の番号。
8	MIME タイプ (<u>M</u> ultipurpose <u>I</u> nternet <u>M</u> ail <u>E</u> xtension)	IANA に登録されている、転送するデータの種類や形式を判別するための識別子。

No	用語	説明
9	TDB 企業コード (Teikoku Data Bank)	帝国データバンクが独自に取材・収集した企業情報に加え、各種公的情報を基に、1社=1コードとして厳格に設定した数字9桁の企業識別コード。
10	耐タンパー性	非正規な手段による外部からの解析が容易に出来ないよう、データの読み取りや改ざんを防ぐ能力。
11	データプロファイル	「平成28年度IoT推進のための社会システム推進事業（スマート工場実証事業）」の成果物であり、水道情報活用システム上でデータをやり取りする際のデータ流通のルール。
12	パディング	決められたデータの長さに対してデータが短い場合に、データを追加してデータの長さを合わせる処理。
13	標準企業コード	一般財団法人日本情報経済社会推進協会(JIPDEC)が一元的に管理する、企業を識別する業界横断的な企業コード。 企業を一意に識別できる6桁の企業識別コードと、各企業が採番、管理を行う6桁の枝番で構成される。
14	ペイロードデータ	パケット通信において、データの転送先や転送経路などを制御するための情報を含むヘッダや、データの破損などを検査するトレーラなどの付加的情報を除いた、ユーザーが送信したいデータ本体。
15	メッセージダイジェスト	任意の長さの文字列を固定長のビット列に変換するアルゴリズム。
16	リダイレクト	ウェブサイトを訪れたユーザーを、自動的に他のウェブページに転送する処理。
17	レルム名	それぞれのレルム(同一の認証ポリシーを適用する範囲)を識別する名称。

1.5 本ドキュメントの記載範囲

本ドキュメントでは、IoT ゲートウェイの外部仕様について記載する。本ドキュメントの記載範囲を以下に示す(図 1-2)。



1.6 本ドキュメントに記載する外部仕様の位置づけ

本ドキュメントに記載する外部仕様は、水道情報活用システムの IoT ゲートウェイとして求められる必須の振る舞いを示したものであり、必要に応じて事業体が追加で求める仕様や機能を、IoT ゲートウェイ・デバイスベンダーが競争領域として独自に構築・提供することを禁ずるものではない。

2. 概要

2.1 IoT ゲートウェイの役割と特徴

IoT ゲートウェイは、デバイスのデータを水道標準プラットフォームにデータ流通するための中継する役割を担う。デバイスのデータを収集し、水道標準プラットフォームの機器ベンダー向け標準インターフェイス(デバイス)で、データをやり取りする。

IoT ゲートウェイが必要とするモジュールについて以下に記載する(表 2-1)。

表 2-1: IoT ゲートウェイのシステム処理機能一覧

No	システム処理機能	説明
1	機器ベンダー向け 標準インターフェイス(デバイス)	標準インターフェイス(デバイス)は、水道標準プラットフォームと IoT ゲートウェイ間でデータをやり取りする機能を提供する。本ドキュメントでは、IoT ゲートウェイ側の機能について記載をする。
2	データセキュリティ	通信データの暗号化/復号、電子署名の検証/付与する機能を提供する。
3	一次データ蓄積	一次データ蓄積は、デバイスから取得したデータをゲートウェイ内に蓄積し、標準インターフェイスの再送要求に応じてデータを提供する機能を提供する。
4	デバイス接続	IoT ゲートウェイとデバイス間でデータをやり取りする機能を提供する。
5	システム監視	ゲートウェイのシステム状態を監視するための機能を提供する。

IoT ゲートウェイのシステム処理機能構成を以下に示す(図 2-1)。

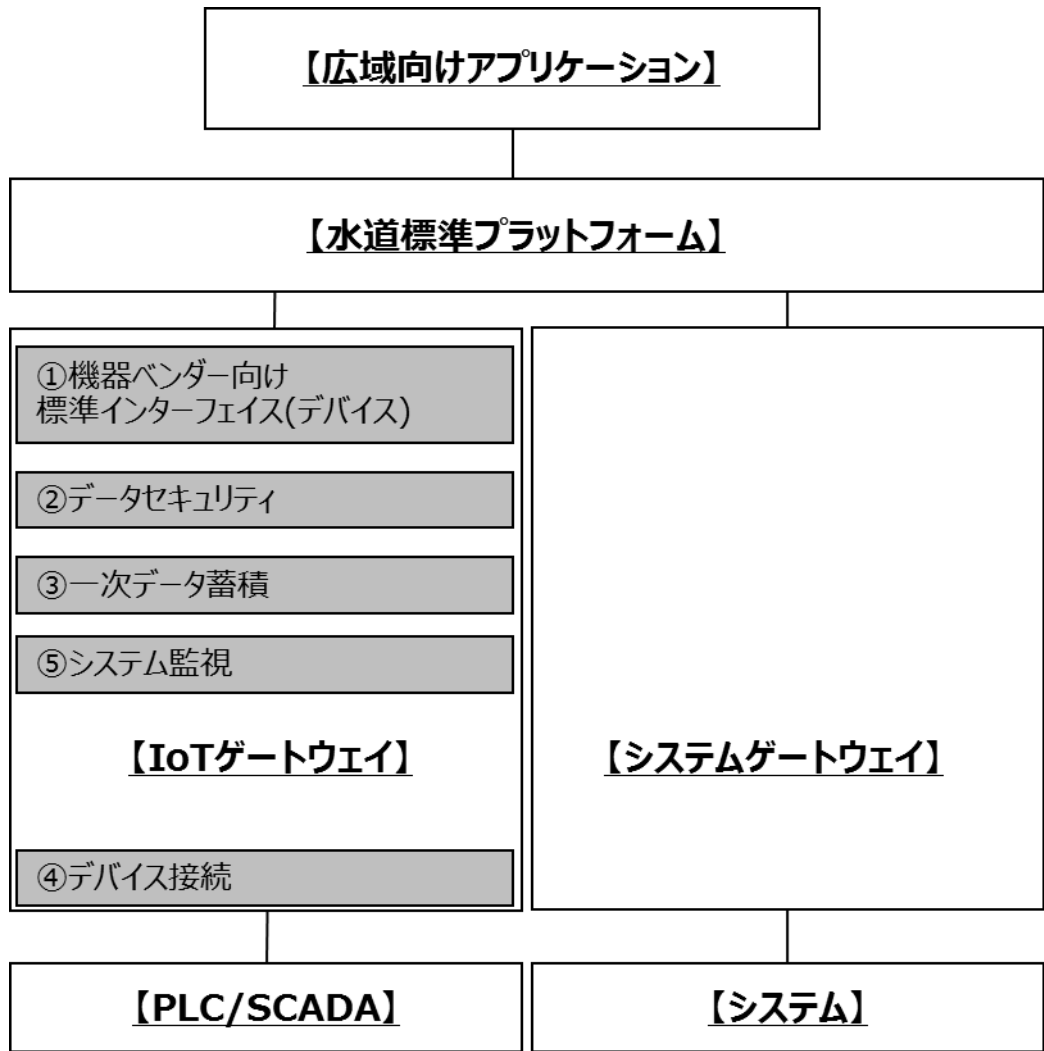


図 2-1: IoT ゲートウェイのシステム処理機能構成

2.2 IoT ゲートウェイの機能における競争領域と協調領域

IoT ゲートウェイは、デバイスのデータを水道標準プラットフォームにデータ流通するための中継する役割を担うものであるため、協調領域となる水道標準プラットフォームと仕様を合わせる必要がある機能が存在し、その機能は「協調領域」として定義される。ただしそれ以外の機能については、IoT ゲートウェイ・デバイスベンダー特有のノウハウで構築することが可能であるため、「競争領域」として定義される。

上記観点を踏まえ、IoT ゲートウェイにおけるシステム処理機能毎の領域の定義は以下（表 2-2）となる。

なお、「協調領域」となる機能においては、プラットフォーマーよりサンプルプログラムが公開される。IoT ゲートウェイ・デバイスベンダーは、これを活用しつつ、全てのシステム処理機能を構築する必要がある。

表 2-2: IoT ゲートウェイのシステム処理機能毎の領域

No	システム処理機能	説明	領域	理由
1	機器ベンダー向け標準インターフェイス(デバイス)	標準インターフェイス(デバイス)は、水道標準プラットフォームと IoT ゲートウェイ間でデータをやり取りする機能を提供する。本ドキュメントでは、IoT ゲートウェイ側の機能について記載をする。	協調領域	水道標準プラットフォームとの通信を行う機能であり、通信仕様は「03_機器ベンダー向け標準インターフェイス(デバイス)仕様書」で示した仕様を実現するため、「協調領域」となる。
2	データセキュリティ	通信データの暗号化/復号、電子署名の検証/付与する機能を提供する。	協調領域	水道標準プラットフォームの「データセキュリティ」と同じ仕様とする必要があるため、「協調領域」となる。
3	一次データ蓄積	一次データ蓄積は、デバイスから取得したデータをゲートウェイ内に蓄積し、標準インターフェイスの再送要求に応じてデータを提供する機能を提供する。	競争領域	水道標準プラットフォームとの通信には影響がなく、IoT ゲートウェイ内に閉じた機能であるため、「競争領域」となる。

4	デバイス接続	IoT ゲートウェイとデバイス間でデータをやり取りする機能を提供する。	競争領域	デバイスはメーカー特有のプロトコルでの通信が必要なケースがほとんどであるため、本機能は都度作り込むものとなり、「競争領域」となる。
5	システム監視	ゲートウェイのシステム状態を監視するための機能を提供する。	協調領域	水道標準プラットフォームの「システム監視」機能により集約監視することが可能であり、そのためには IoT ゲートウェイでも同じ仕様の機能を構築する必要があるため、協調領域」とする。

3. 機器ベンダー向け標準インターフェイス(デバイス)モジュール

3.1 機能概要

標準インターフェイス(デバイス)は、水道標準プラットフォームと IoT ゲートウェイ間でデータをやり取りする機能を提供する。

3.2 機能一覧

本機能におけるモジュール機能の一覧を示す(図 3-1、表 3-1)。

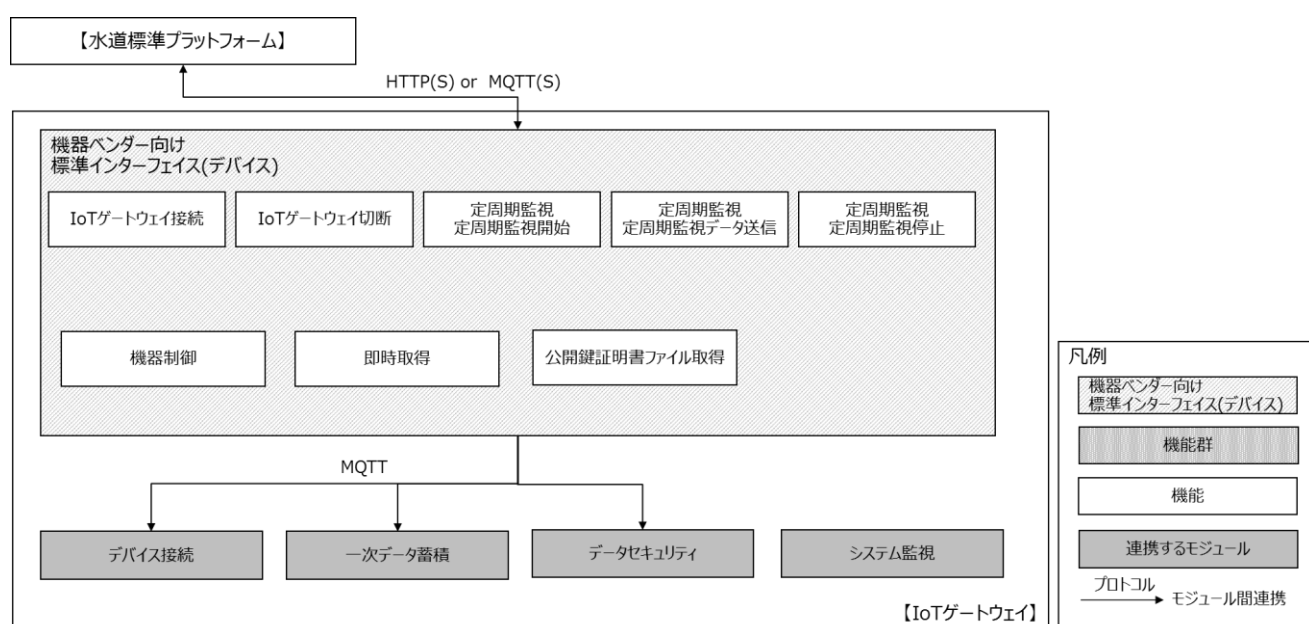


図 3-1: 機器ベンダー向け標準インターフェイス(デバイス)の機能(モジュール)構成

表 3-1: 機器ベンダー向け標準インターフェイス(デバイス)機能一覧

No	機能	概要説明
1	IoT ゲートウェイ接続	IoT ゲートウェイを水道標準プラットフォームに接続する処理を行う
2	IoT ゲートウェイ切断	IoT ゲートウェイを水道標準プラットフォームから切断する処理を行う
3	定周期監視	水道標準プラットフォームに対し、定周期で計測対象データを送付する機能
4	定周期監視開始	水道標準プラットフォームからの要求に従って、定周期監視を開始する処理を行う
5	定周期監視データ送信	デバイス接続から定周期監視の計測対象データを受領し、水道標準プラットフォームへ送付する処理を行う

No	機能	概要説明
6	定周期監視停止	水道標準プラットフォームからの要求に従って、定周期監視を停止する処理を行う
7	即時取得	水道標準プラットフォームからの要求に従って、計測対象データを送付する処理を行う
8	機器制御	水道標準プラットフォームからの要求に従って、機器制御を行う
9	公開鍵証明書ファイル取得	アプリケーション証明書(データ保護用)、水道標準プラットフォーム証明書(データ保護用)を取得する処理を行う

3.3 機能要件

3.3.1 IoT ゲートウェイ接続

(1) 機能概要

IoT ゲートウェイを水道標準プラットフォームに接続する処理を行う。

- ・ 水道標準プラットフォームに、ゲートウェイ接続情報を含んだゲートウェイ接続要求を送信する。
- ・ 水道標準プラットフォームから、ゲートウェイ接続結果を受信する。

(2) 提供経路

機能を提供する経路を以下に図示する(図 3-2)。

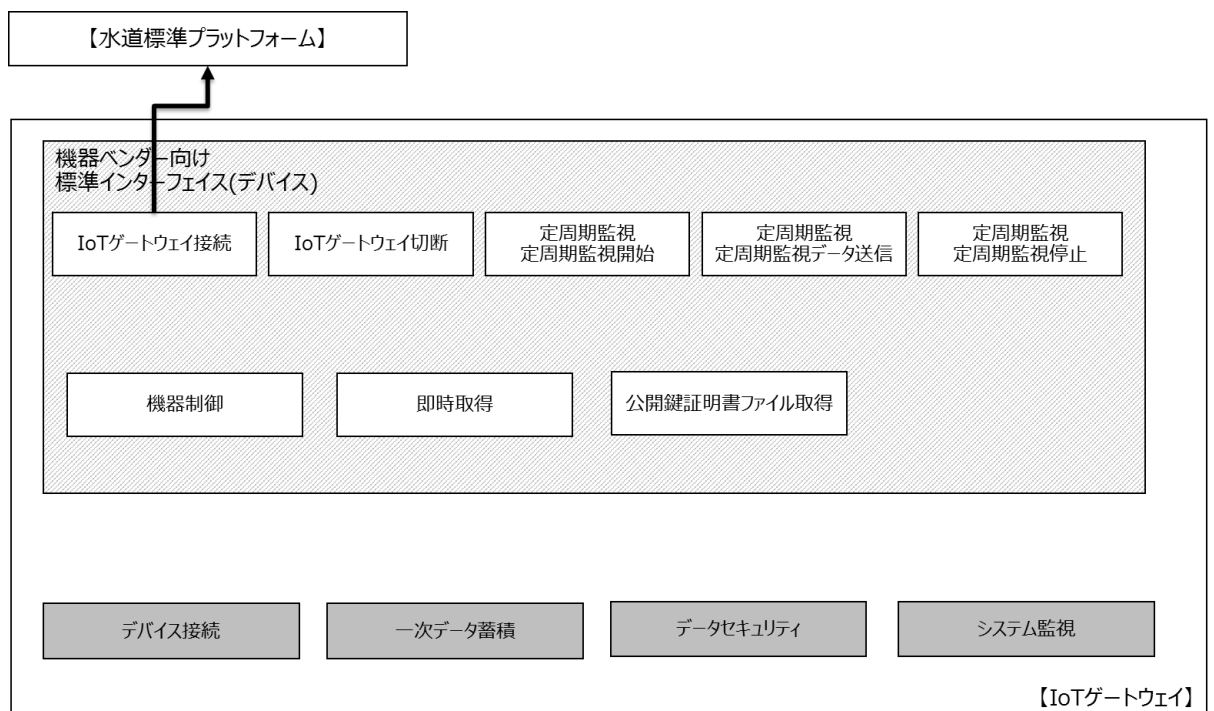


図 3-2: IoT ゲートウェイ接続機能 提供経路

3.3.2 IoT ゲートウェイ切断

(1) 機能概要

IoT ゲートウェイを水道標準プラットフォームに切断する処理を行う。

- ・ 水道標準プラットフォームに、ゲートウェイ切断情報を含んだゲートウェイ切断要求を送信する。
- ・ 水道標準プラットフォームから、ゲートウェイ切断結果を受信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 3-3)。

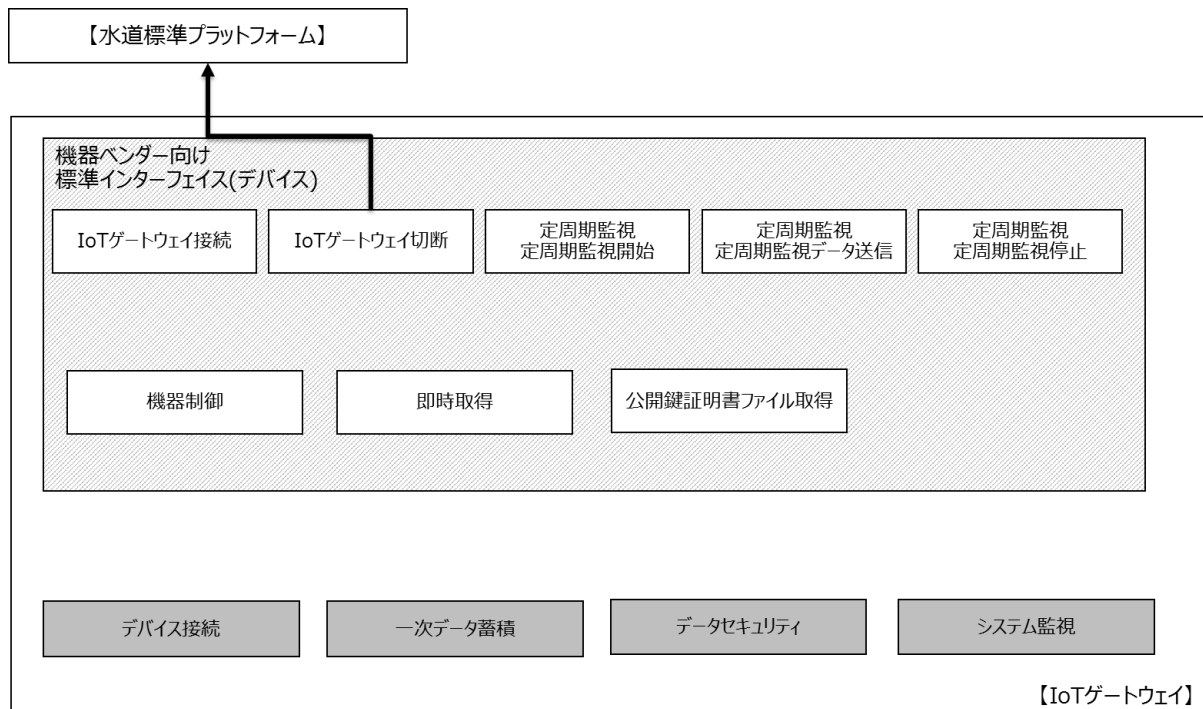


図 3-3: IoT ゲートウェイ切断機能 提供経路

3.3.3 定周期監視-定周期監視開始

(1) 機能概要

水道標準プラットフォームからの要求に従って、定周期監視を開始する処理を行う。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 3-4)。

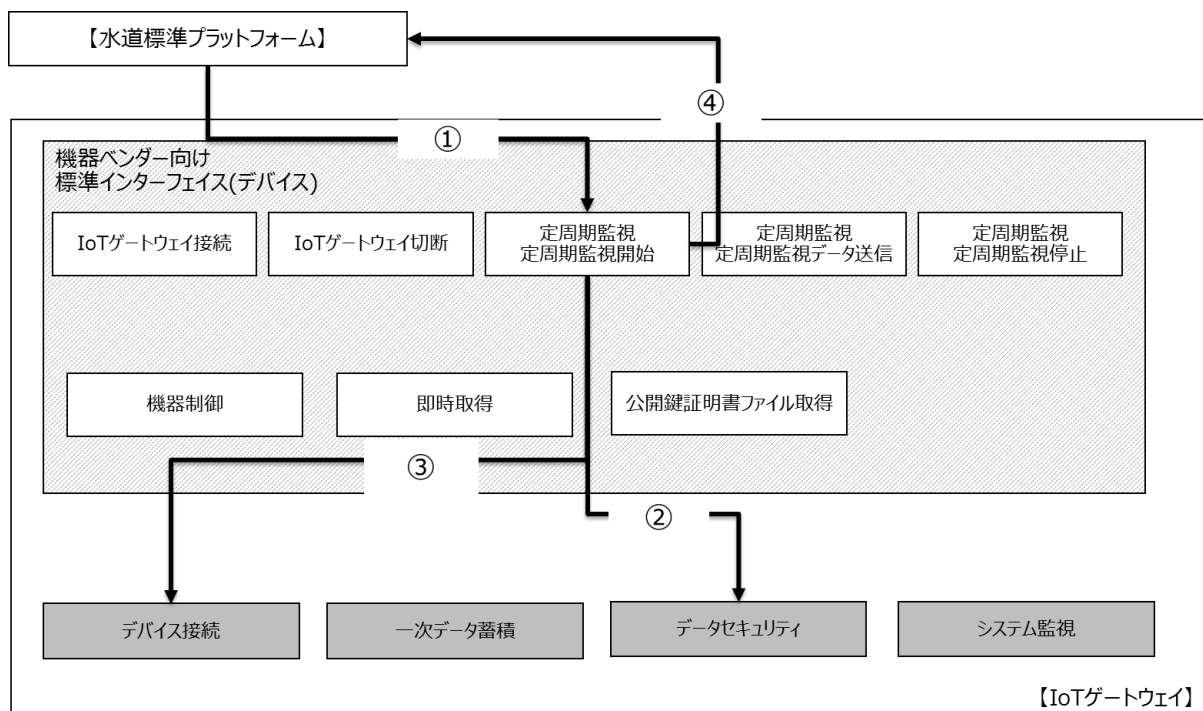


図 3-4: 定周期監視-定周期監視開始機能 提供経路

処理概要は以下の通り(表 3-2)。

表 3-2: 定周期監視-定周期監視開始機能 処理概要

No	処理概要
1	水道標準プラットフォームから定周期監視開始要求を受信する。
2	定周期監視-定周期監視開始機能からデータセキュリティモジュールに電子署名検証機能、データ復号機能実行を要求し、電子署名検証結果と復号データを受信する。
3	定周期監視-定周期監視開始機能からデバイス接続に定周期監視開始要求を送信し、定周期監視開始要求結果を受信する。
4	定周期監視-定周期監視開始機能から水道標準プラットフォームに定周期監視開始要求結果を送信し、定周期監視開始要求通信結果を受信する。

3.3.4 定周期監視-定周期監視データ送信

(1) 機能概要

デバイス接続から定周期監視の計測対象データを受領し、水道標準プラットフォームへ送付する処理を行う。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 3-5)。

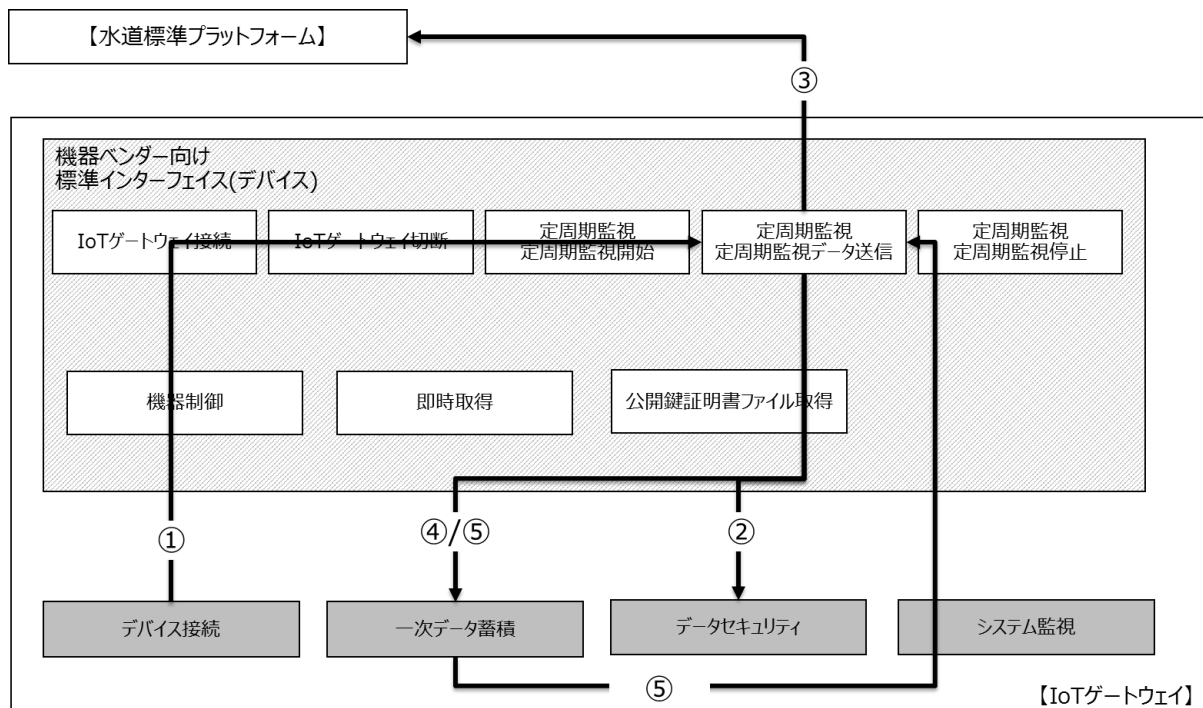


図 3-5: 定周期監視-定周期監視データ送信 提供経路

処理概要は以下の通り(表 3-3)。

表 3-3: 定周期監視-定周期監視データ送信機能 処理概要

No	処理概要
1	デバイス接続から定周期監視データ送信要求を受信する。
2	定周期監視-定周期監視データ送信機能からデータセキュリティモジュールに電子署名付与機能、データ暗号化機能実行を要求し、電子署名を付与された暗号化データを受信する。
3	定周期監視-定周期監視データ送信機能から水道標準プラットフォームに定周期監視データを送信する。水道標準プラットフォームから定周期監視データ送信通信結果を受信する。
4	定周期監視-定周期監視データ送信機能から一次データ蓄積に定周期監視データを送信する。
5	定周期監視データ送信が失敗した場合、定周期監視-定周期監視データ送信機能から一次データ蓄積にデータ提供機能実行を要求し、再送処理用の定周期監視データを取得する。一次データ蓄積からデータ提供機能実行結果を受信し、再送処理を行う。

3.3.5 定周期監視-定周期監視停止

(1) 機能概要

水道標準プラットフォームからの要求に従って、定周期監視を停止する処理を行う。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 3-6)。

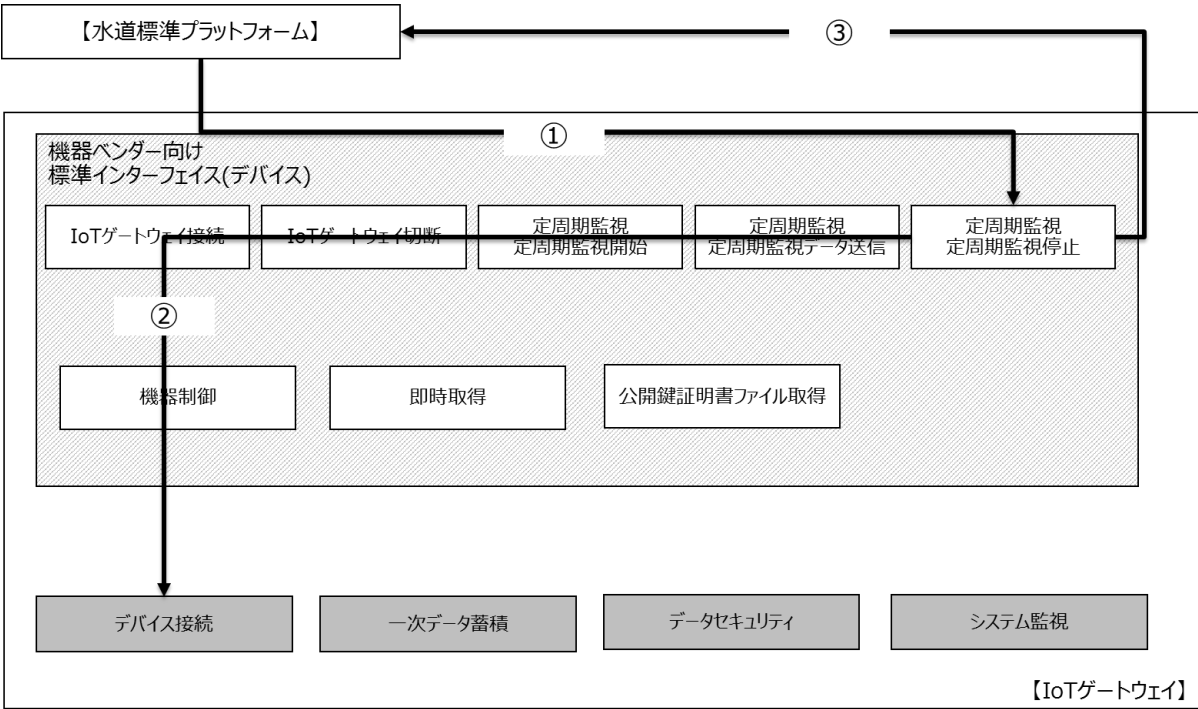


図 3-6: 定周期監視-定周期監視停止 提供経路

処理概要は以下の通り(表 3-4)。

表 3-4: 定周期監視-定周期監視停止機能 処理概要

No	処理概要
1	水道標準プラットフォームから定周期監視停止要求を受信する。
2	定周期監視-定周期監視停止機能からデバイス接続に定周期監視停止要求を送信し、デバイス接続から定周期監視停止要求結果を受信する。
3	定周期監視-定周期監視停止機能から水道標準プラットフォームに定周期監視停止要求結果を送信し、水道標準プラットフォームから定周期監視停止要求通信結果を受信する。

3.3.6 即時取得

(1) 機能概要

水道標準プラットフォームからの要求に従って、計測対象データを送付する処理を行う。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 3-7)。

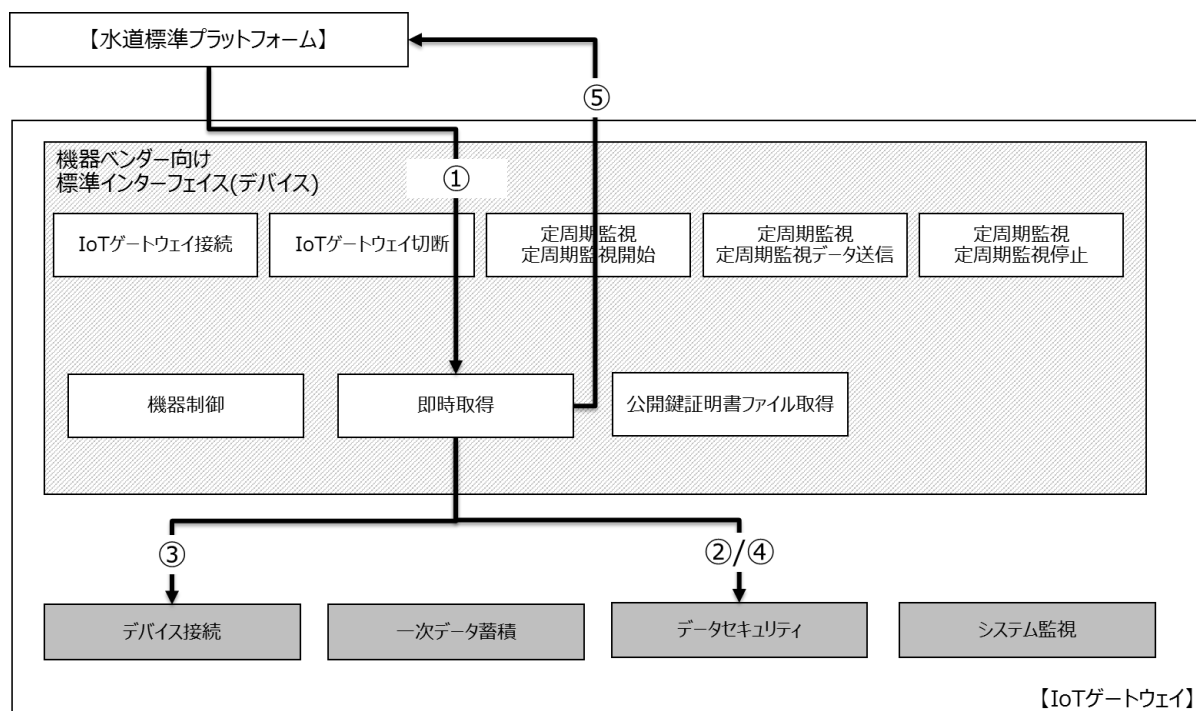


図 3-7: 即時取得機能 提供経路

処理概要は以下の通り(表 3-5)。

表 3-5: 即時取得機能 処理概要

No	処理概要
1	水道標準プラットフォームから即時取得要求を受信する。
2	即時取得機能からデータセキュリティに電子署名検証機能、データ復号機能実行を要求し、電子署名検証結果と復号データを受信する。
3	即時取得機能からデバイス接続に即時取得要求を送信する。デバイス接続から即時取得要求結果を受信する。
4	即時取得機能からデータセキュリティにデータ暗号化機能、電子署名付与機能実行を要求し、電子署名を付与された暗号化データを受信する。
5	即時取得機能から水道標準プラットフォームに、即時取得結果を送信する。 水道標準プラットフォームから即時取得通信結果を受信する。

3.3.7 機器制御

(1) 機能概要

水道標準プラットフォームからの要求に従って、制御操作を行う。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 3-8)。

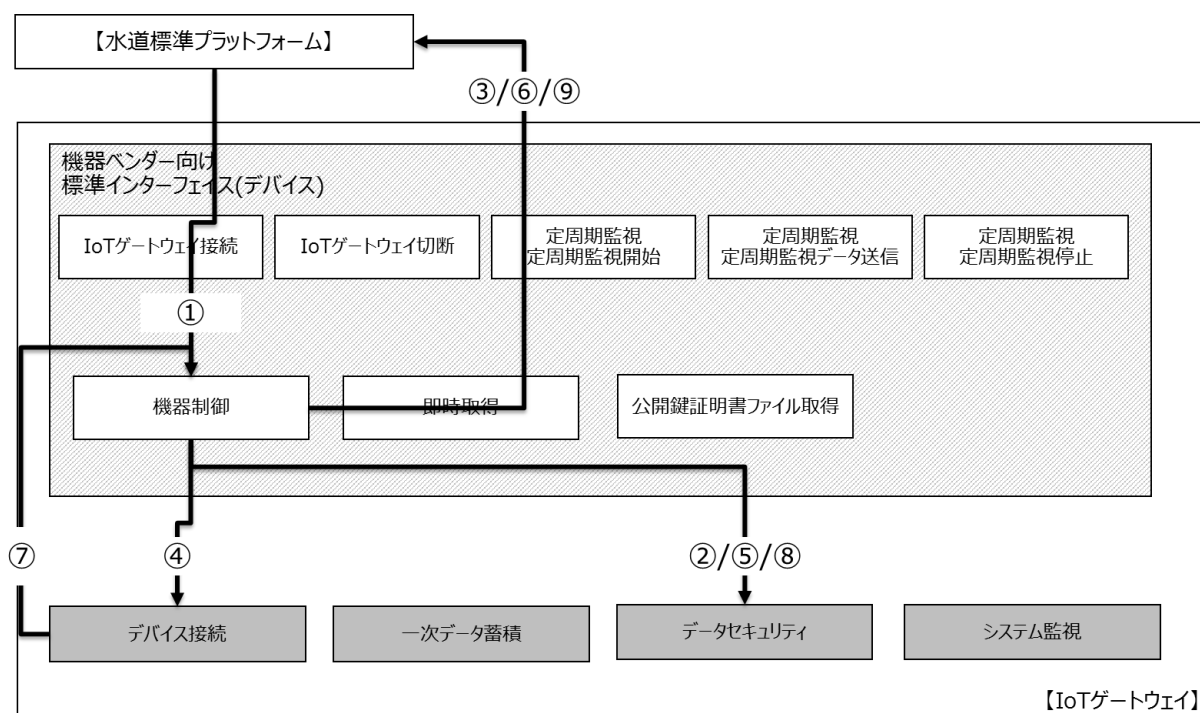


図 3-8: 機器制御機能 提供経路

処理概要は以下の通り(表 3-6)。

表 3-6: 機器制御機能 処理概要

No	処理概要
1	水道標準プラットフォームから制御操作要求を受信する。
2	機器制御機能からデータセキュリティに電子署名検証機能、データ復号機能実行を要求し、電子署名検証結果と復号データを受信する。
3	機器制御機能から水道標準プラットフォームに制御操作要求送達完了通知を送信する。
4	機器制御機能からデバイス接続に制御操作要求を送信し、制御操作要求完了通知を受信する。
5	機器制御機能からデータセキュリティにデータ暗号化機能、電子署名付与機能実行を要求し、電子署名を付与された暗号化データを受信する。
6	機器制御機能から水道標準プラットフォームに制御操作要求完了通知を送信する。
7	デバイス接続から制御操作完了通知を受信する。

No	処理概要
8	機器制御機能からデータセキュリティにデータ暗号化機能、電子署名付与機能実行を要求し、電子署名を付与された暗号化データを受信する。
9	機器制御機能から水道標準プラットフォームに制御操作完了通知を送信する。

3.3.8 公開鍵証明書ファイル取得

(1) 機能概要

アプリケーション証明書(データ保護用)、水道標準プラットフォーム証明書(データ保護用)を取得する処理を行う。

- ・ 公開鍵証明書ファイル取得機能から水道標準プラットフォームにデータ保護用公開鍵証明書ファイル取得要求を送信する。
- ・ 水道標準プラットフォームからデータ保護用公開鍵証明書ファイル取得要求結果を受信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 3-9)。

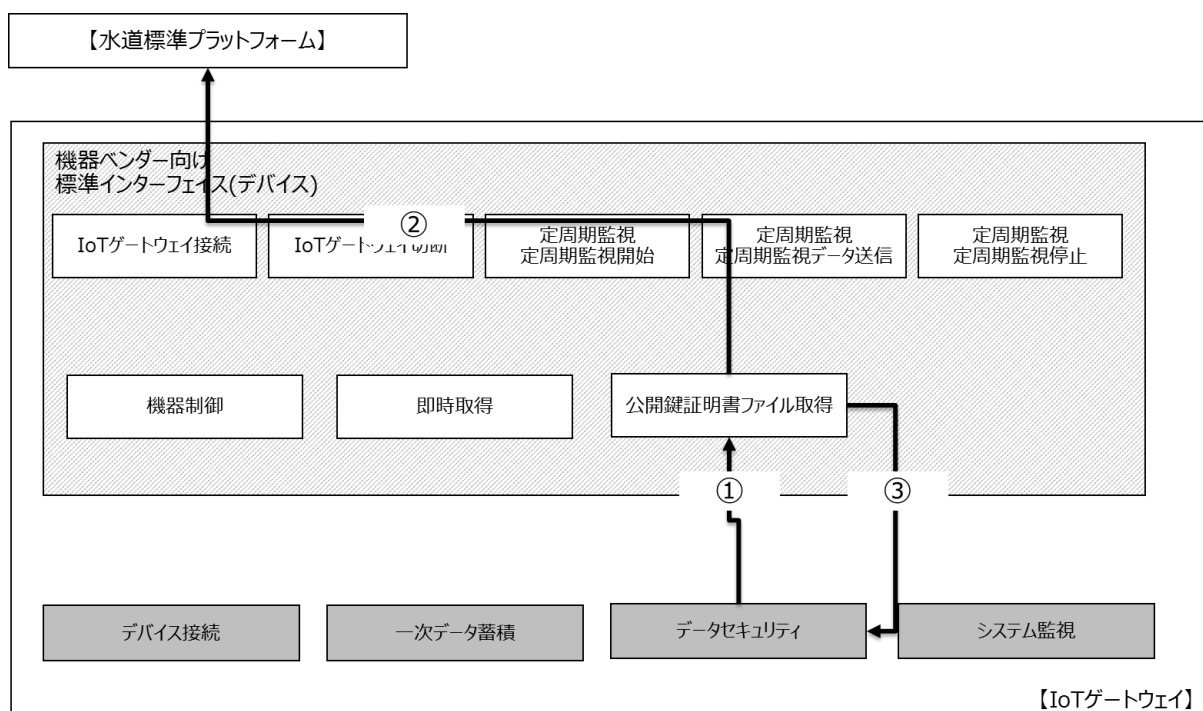


図 3-9: 公開鍵証明書ファイル機能 提供経路

処理概要は以下の通り(表 3-7)。

表 3-7: 即時取得機能 処理概要

No	処理概要
1	データセキュリティからデータ保護用公開鍵証明書ファイル取得要求を受信する。
2	公開鍵証明書ファイル取得機能から水道標準プラットフォームにデータ保護用公開鍵証明書ファイル取得要求を送信し、データ保護用証明書ファイルを受信する。
3	公開鍵証明書ファイル取得機能からデータセキュリティへデータ保護用証明書ファイルを送信する。

4. データセキュリティモジュール

4.1 機能概要

通信データの暗号化/復号、電子署名の検証/付与する機能を提供する。

4.1.1 機能一覧

本機能におけるモジュール機能の一覧を示す(図 4-1、表 4-1)。

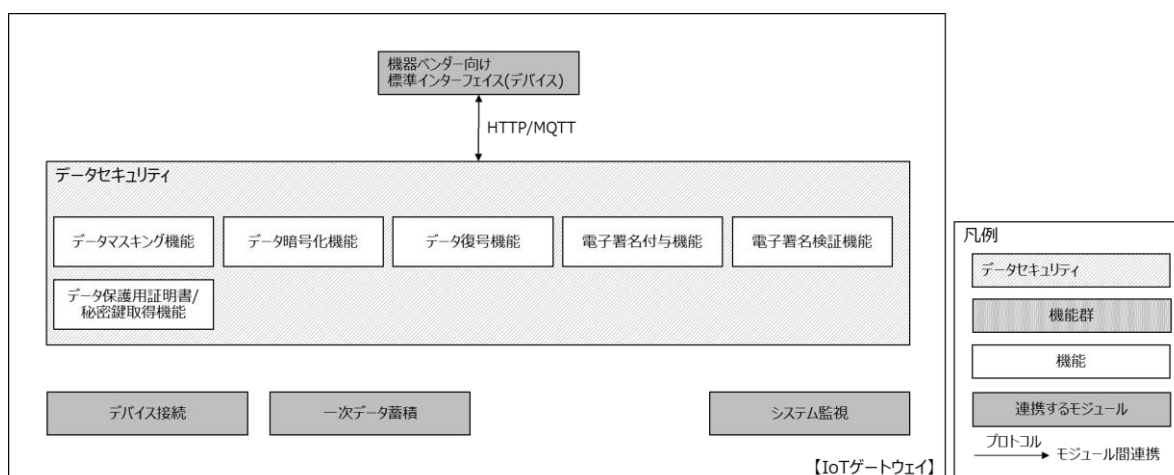


図 4-1: データセキュリティ機能(モジュール)構成

表 4-1: データセキュリティ機能一覧

No	機能	概要説明
1	データ保護用証明書/ 秘密鍵取得機能	機器ベンダー向け標準インターフェイス(デバイス)を通じて水道標準プラットフォームから、アプリケーション証明書(データ保護用)、水道標準プラットフォーム証明書(データ保護用)を取得する
2	データ暗号化機能	機器ベンダー向け標準インターフェイス(デバイス)の要求に対し、通信データの暗号化を実施する
3	データ復号機能	機器ベンダー向け標準インターフェイス(デバイス)の要求に対し、通信データの復号を実施する
4	電子署名付与機能	機器ベンダー向け標準インターフェイス(デバイス)の要求に対し、通信データの電子署名を付与する
5	電子署名検証機能	機器ベンダー向け標準インターフェイス(デバイス)の要求に対し、通信データの電子署名を検証する
6	データマスキング機能	事業体用秘密鍵を用いて、既存システムの任意のデータ項目をマスキングする。

4.1.2 データ暗号化/データ復号方式

データセキュリティにおけるデータの暗号化/復号方式は、データ形式に応じた以下の方式とする。

(1) データプロファイル(XML)形式

(a) 概要

データプロファイル(XML)形式のデータの暗号化/復号方式は、以下に図示した手順で実施する(図 4-2、図 4-3)。

【送信側での暗号化処理方式】

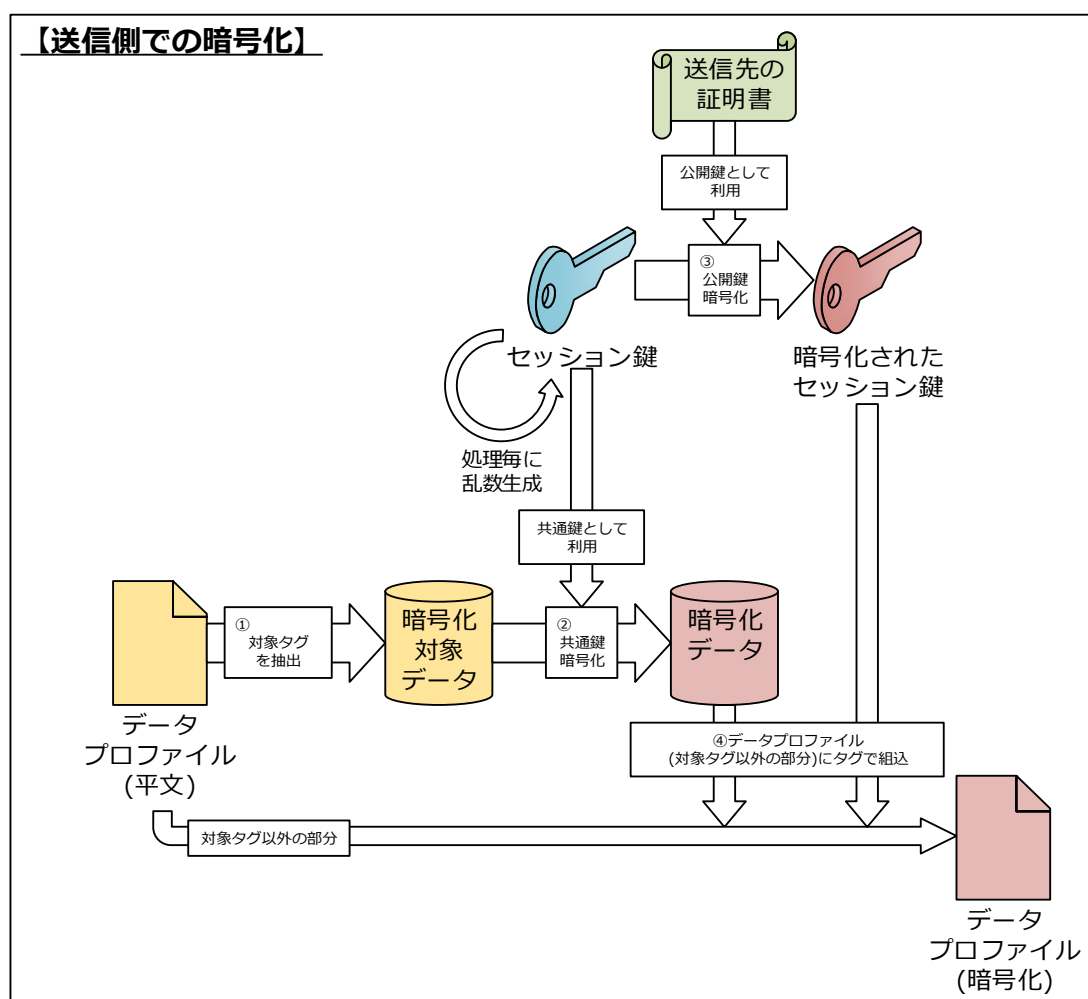


図 4-2:送信側での暗号化処理方式

- ① 「データプロファイル(平文)」から対象のタグを「暗号化対象データ」として抽出する。
- ② 処理毎に乱数生成した「セッション鍵」を共通鍵として、①で抽出した「暗号化対象データ」を共通鍵暗号方式で暗号化し、「暗号化データ」を生成する。
- ③ 「送信先の証明書」を公開鍵として、②で利用した「セッション鍵」を公開鍵暗号方式で暗号化し、「暗号化されたセッション鍵」を生成する。

- ④ ②と③で生成した「暗号化データ」と「暗号化されたセッション鍵」をデータプロフィール(対象タグ以外の部分)にタグで組み込んで、「データプロフィール(暗号化)」を生成する。

【受信側での復号処理方式】

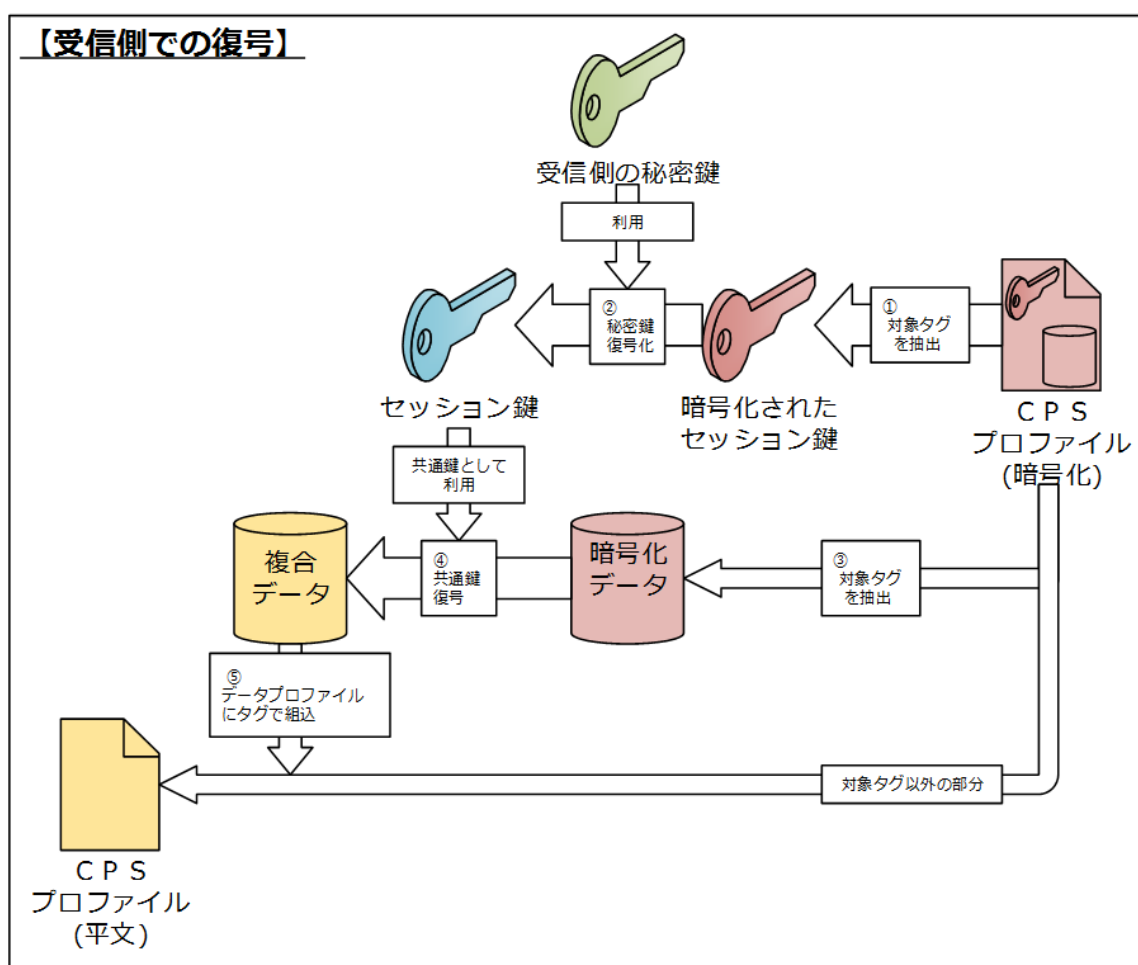


図 4-3:受信側での復号処理方式

- ① 「データプロフィール(暗号化)」から対象のタグを「暗号化されたセッション鍵」として抽出する。
- ② 「受信側の秘密鍵」を利用して、①で抽出した「暗号化されたセッション鍵」を復号し、「セッション鍵」を生成する。
- ③ 「データプロフィール(暗号化)」から対象のタグを「暗号化データ」として抽出する。
- ④ ②で生成した「セッション鍵」を利用して、③で抽出した「暗号化データ」を復号し、「復号データ」を生成する。
- ⑤ で生成した「復号データ」データプロフィール(対象タグ以外の部分)にタグで組み込んで、「データプロフィール(平文)」を生成する。

(b) 暗号アルゴリズム

① 共通鍵暗号方式

データを暗号化/復号する暗号アルゴリズムを以下に示す(表 4-2)。

表 4-2: 共通鍵暗号方式の暗号アルゴリズム

No	区分	方式
1	暗号アルゴリズム	AES
2	暗号モード	CBC
3	鍵長	128bit, 192bit, 256bit から選択
4	ブロック長	128bit
5	パディング	PKCS#7

② 公開鍵暗号方式

データの暗号化/復号に利用するセッション鍵を暗号化/復号する暗号アルゴリズムを以下に示す(表 4-3)。

表 4-3: 公開鍵暗号方式の暗号アルゴリズム

No	区分	方式
1	暗号アルゴリズム	RSA
2	鍵長	2048bit
3	ブロック長	2048bit
4	パディング	OAEP

(2) データプロファイル(JSON)形式

(a) 概要

データプロファイル(JSON)形式のデータの暗号化/復号方式は、RFC7516 準拠し以下に図示した手順で実施する(図 4-4、図 4-5)。

【送信側での暗号化処理方式】

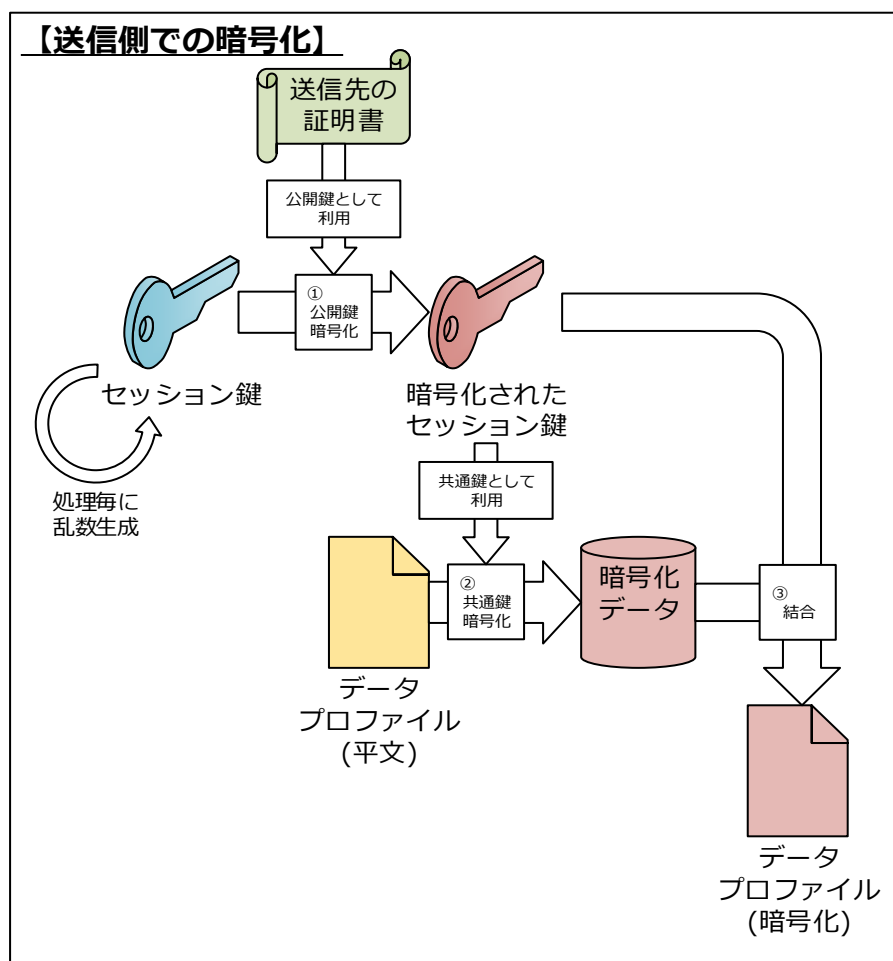


図 4-4: 送信側での暗号化処理方式

- ① 「送信先の証明書」を公開鍵として、処理毎に乱数生成した「セッション鍵」を公開鍵暗号方式で暗号化し、「暗号化されたセッション鍵」を生成する。
- ② ①で生成した「暗号化されたセッション鍵」を共通鍵として、「データプロファイル(平文)」を共通鍵暗号方式で暗号化し、「暗号化データ」を生成する。
- ③ ①で生成した「暗号化されたセッション鍵」と②で生成した「暗号化データ」を結合して、「データプロファイル(暗号化)」を生成する。

【受信側での復号処理方式】

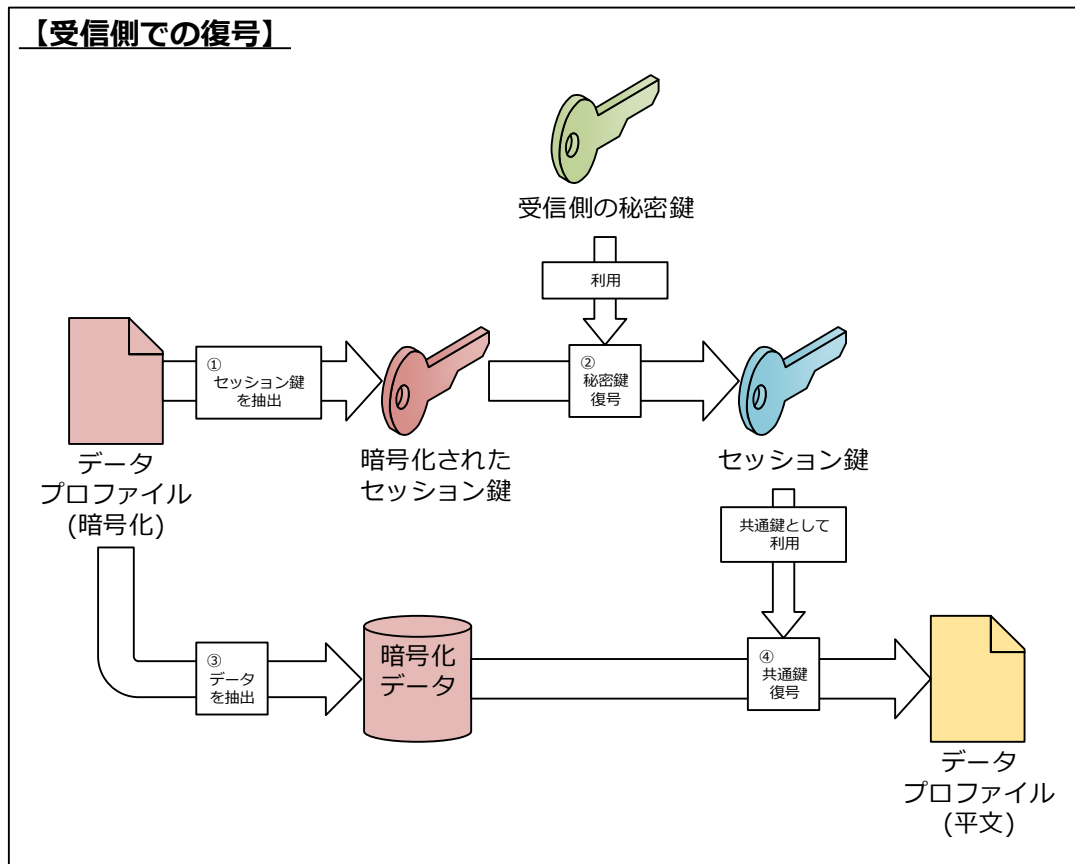


図 4-5: 受信側での復号処理方式

- ① 「データプロファイル(暗号化)」から「暗号化されたセッション鍵」を抽出する。
- ② 「受信側の秘密鍵」を利用して、①で抽出した「暗号化されたセッション鍵」を復号し、「セッション鍵」を生成する。
- ③ 「データプロファイル(暗号化)」から「暗号化データ」を抽出する。
- ④ ②で生成した「セッション鍵」を利用して、③で抽出した「暗号化データ」を復号し、「データプロファイル(平文)」を生成する。

(b) 暗号アルゴリズム

① 共通鍵暗号方式

データを暗号化/復号する暗号アルゴリズムを以下に示す(表 4-4)。

表 4-4: 共通鍵暗号方式の暗号アルゴリズム

No	区分	方式
1	暗号アルゴリズム	AES
2	暗号モード	CBC
3	鍵長	128bit
4	ブロック長	128bit
5	パディング	PKCS#7
6	メッセージダイジェスト	SHA-256
7	メッセージ認証コード	HMAC

② 公開鍵暗号方式

データの暗号化/復号に利用するセッション鍵を暗号化/復号する暗号アルゴリズムを以下に示す(表 4-5)。

表 4-5: 公開鍵暗号方式の暗号アルゴリズム

No	区分	方式
1	暗号アルゴリズム	RSA
2	鍵長	2048bit
3	ブロック長	2048bit
4	パディング	OAEP

(3) ファイル形式

(a) 概要

ファイル形式のデータの暗号化/復号方式は、以下に図示した手順で実施する(図 4-6: 送信側での暗号化処理方式図 4-6、図 4-7)。

【送信側での暗号化処理方式】

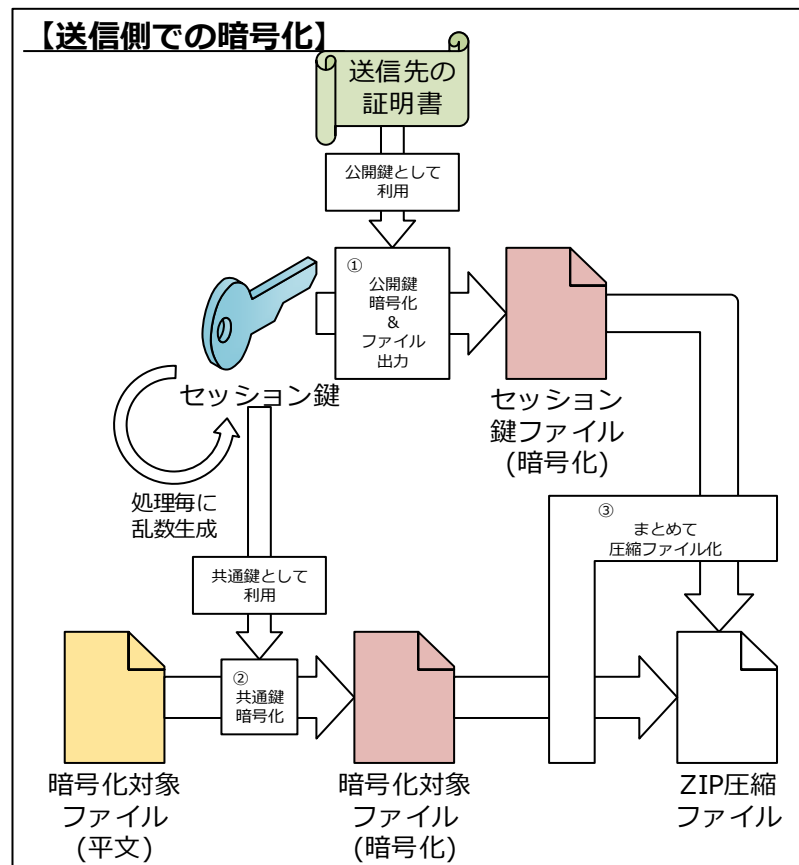


図 4-6: 送信側での暗号化処理方式

- ① 「送信先の証明書」を公開鍵として、処理毎に乱数生成した「セッション鍵」を公開鍵暗号方式で暗号化し、「セッション鍵ファイル(暗号化)」を生成する。
- ② ①で生成した「セッション鍵」を共通鍵として、「暗号化対象ファイル(平文)」を共通鍵暗号方式で暗号化し、「暗号化対象ファイル(暗号化)」を生成する。
- ③ ①で生成した「セッション鍵ファイル(暗号化)」と②で生成した「暗号化対象ファイル(暗号化)」をまとめて圧縮し、「ZIP 圧縮ファイル」を生成する。

【受信側での復号処理方式】

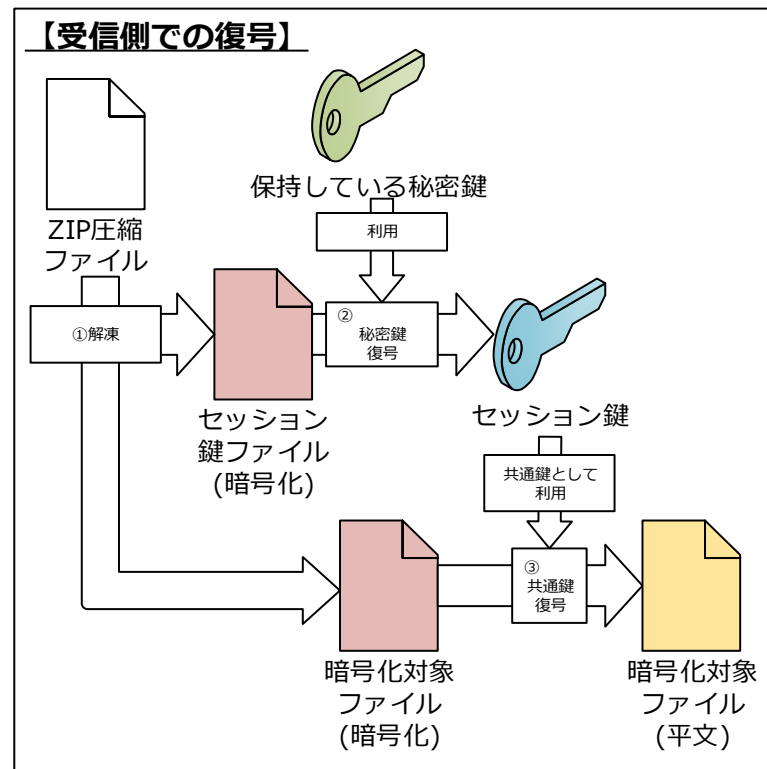


図 4-7:受信側での復号処理方式

- ① 「ZIP 圧縮ファイル」を解凍し、「セッション鍵ファイル(暗号化)」と「暗号化対象ファイル(暗号化)」を抽出する。
- ② 「保持している秘密鍵」を利用して、①で抽出した「セッション鍵ファイル(暗号化)」を復号し、「セッション鍵」を生成する。
- ③ ②で生成した「セッション鍵」を利用して、①で抽出した「暗号化対象ファイル(暗号化)」を復号し、「暗号化対象ファイル(平文)」を生成する。

(b) 暗号アルゴリズム

① 共通鍵暗号方式

データを暗号化/復号する暗号アルゴリズムを以下に示す(表 4-6)。

表 4-6: 共通鍵暗号方式の暗号アルゴリズム

No	区分	方式
1	暗号アルゴリズム	AES
2	暗号モード	CBC
3	鍵長	128bit, 192bit, 256bit から選択
4	ブロック長	128bit
5	パディング	PKCS#7

② 公開鍵暗号方式

データの暗号化/復号に利用するセッション鍵を暗号化/復号する暗号アルゴリズムを以下に示す(表 4-7)。

表 4-7: 公開鍵暗号方式の暗号アルゴリズム

No	区分	方式
1	暗号アルゴリズム	RSA
2	鍵長	2048bit
3	ブロック長	2048bit
4	パディング	OAEP

4.1.3 電子署名方式

データセキュリティにおけるデータの電子署名方式は、データ形式に応じた以下の方式とする。

(1) データプロファイル(XML)形式

(a) 概要

データプロファイル(XML)形式の電子署名付与/検証方式は、以下に図示した手順で実施する。(図 4-8、図 4-9)

【送信側での電子署名付与方式】

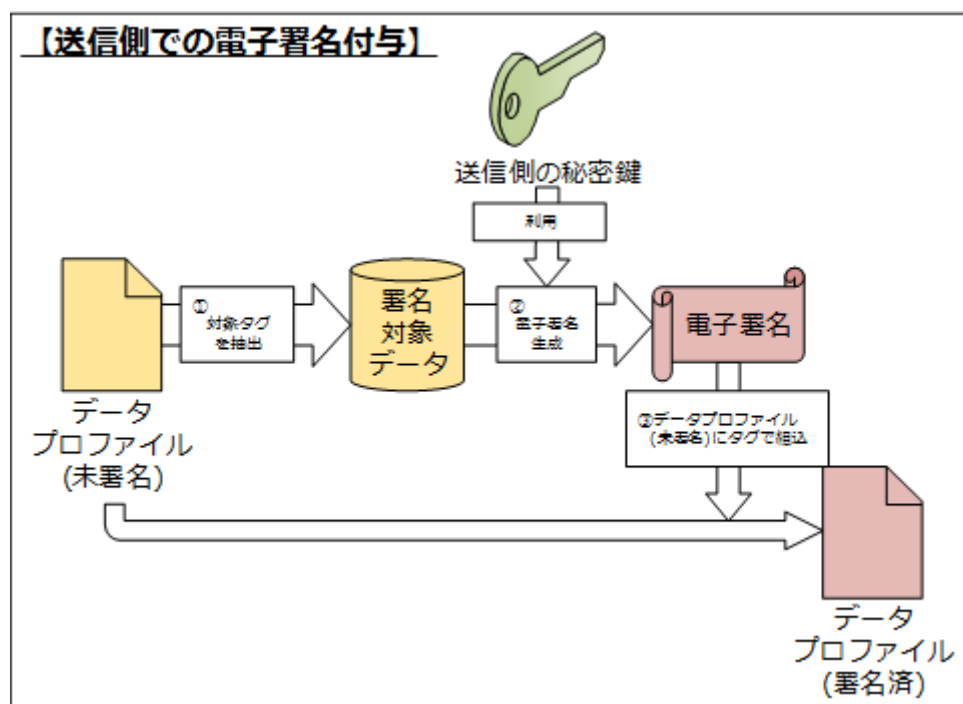


図 4-8: 送信側での電子署名付与方式

- ① 「データプロファイル(未署名)」から対象のタグを「署名対象データ」として抽出する。
- ② ①で抽出した「署名対象データ」と「送信側の秘密鍵」を利用して、「電子署名」を生成する。
- ③ ②で生成した「電子署名」をデータプロファイル(未署名)にタグで組み込んで、「データプロファイル(署名済み)」を生成する。

【受信側での電子署名検証方式】

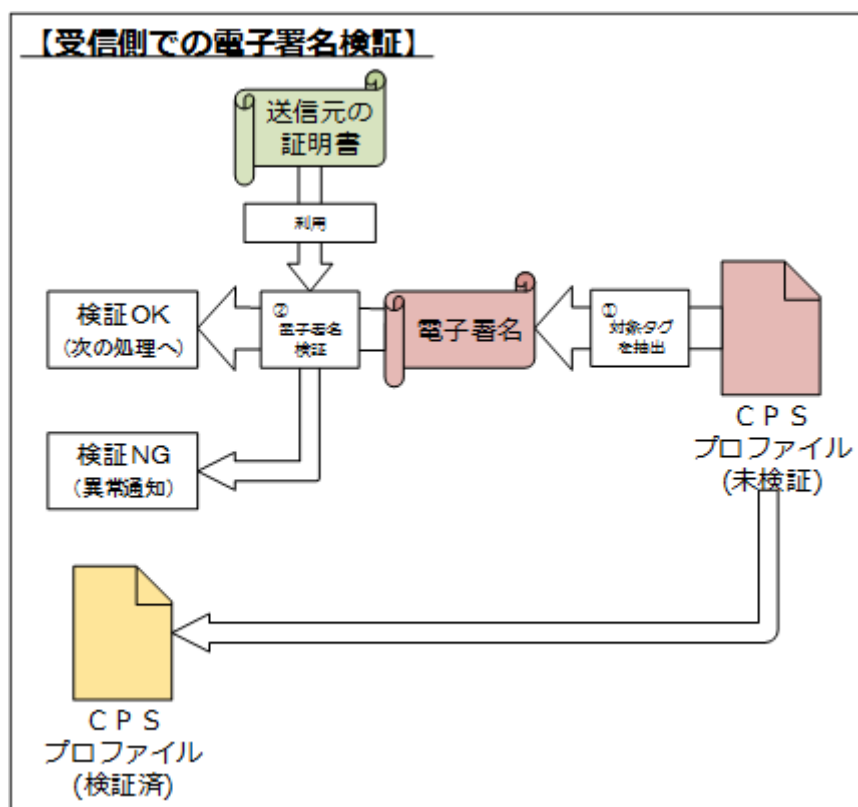


図 4-9:受信側での電子署名検証方式

- ① 「データプロファイル(未検証)」から対象のタグを「電子署名」として抽出する。
- ② 「送信元の証明書」を利用して、①で抽出した「電子署名」を検証し、検証 OK であれば次の処理を実行する。(検証 NG の場合は、異常を通知する。)

(b) 電子署名アルゴリズム

電子署名付与/検証に利用する電子署名アルゴリズムを以下に示す(表 4-8)。

表 4-8: 電子署名アルゴリズム

No	区分	方式
1	正規化	Exclusive XML Canonicalization Version 1.0 (omit comments)
2	署名	RSASSA-PKCS1-v1_5
3	メッセージダイジェスト	SHA-256
4	メッセージ認証コード	HMAC

(2) データプロファイル(JSON)形式

(a) 概要

データプロファイル(JSON)形式の電子署名付与/検証方式は、以下に図示した手順で実施する。(図 4-10、図 4-11)

【送信側での電子署名付与方式】

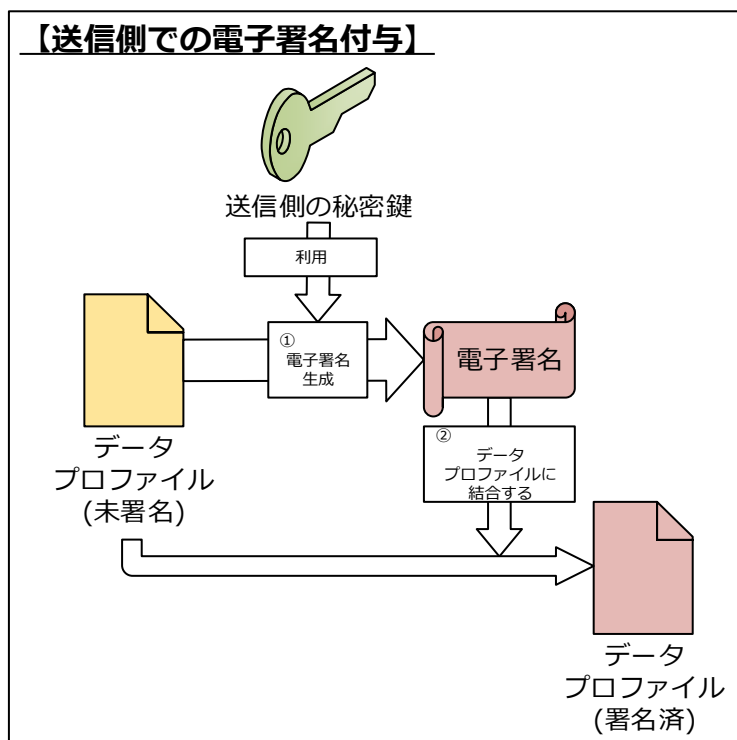


図 4-10: 送信側での電子署名付与方式

- ① 「データプロファイル(未署名)」を参照して送信側の秘密鍵を利用して、「電子署名」を生成する。
- ② ①で生成した「電子署名」と「データプロファイル(未署名)」を結合し、「データプロファイル(署名済)」を生成する。

【受信側での電子署名検証方式】

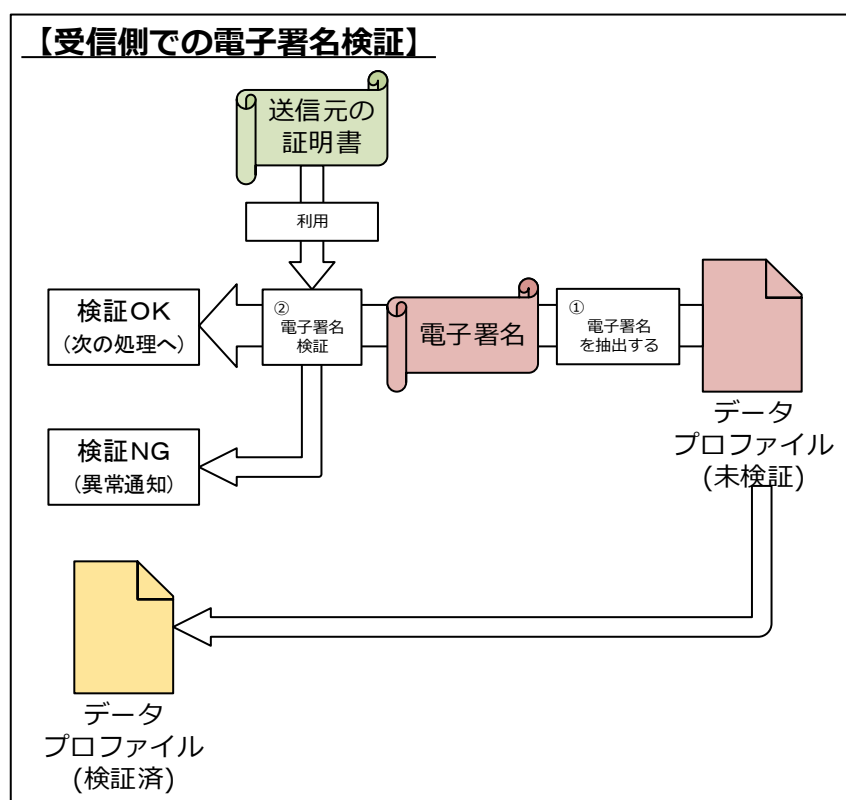


図 4-11:受信側での電子署名検証方式

- ① 「データプロファイル(未検証)」から「電子署名」を抽出する。
- ② 「送信元の証明書」を利用して、「電子署名」を検証し、OKであれば次の処理を実行する。(検証NGの場合は、異常を通知する。)

(b) 電子署名アルゴリズム

電子署名付与/検証に利用する電子署名アルゴリズムを以下に示す(表 4-9)。

表 4-9: 電子署名アルゴリズム

No	区分	方式
1	結合方法	JWS Compact Serialization
2	署名	RSASSA-PKCS1-v1_5
3	メッセージダイジェスト	SHA-256
4	メッセージ認証コード	HMAC

(3) ファイル形式

(a) 概要

ファイル形式の電子署名付与/検証方式は、以下に図示した手順で実施する。(図 4-12、図 4-13)

【送信側での電子署名付与方式】

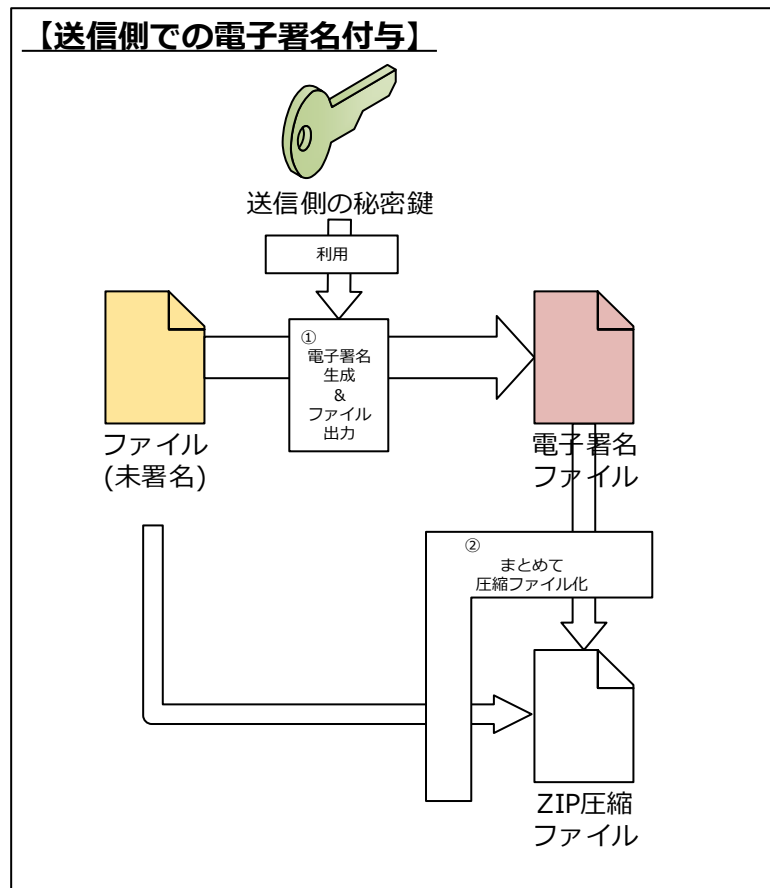


図 4-12: 送信側での電子署名付与方式

- ① 「ファイル(未署名)」を参照し、送信側の秘密鍵を利用して「電子署名ファイル」を生成、ファイル出力する。
- ② ①で生成した「電子署名ファイル」と「データプロファイル(未署名)」をまとめて圧縮し、「ZIP 圧縮ファイル」を生成する。

【受信側での電子署名検証方式】

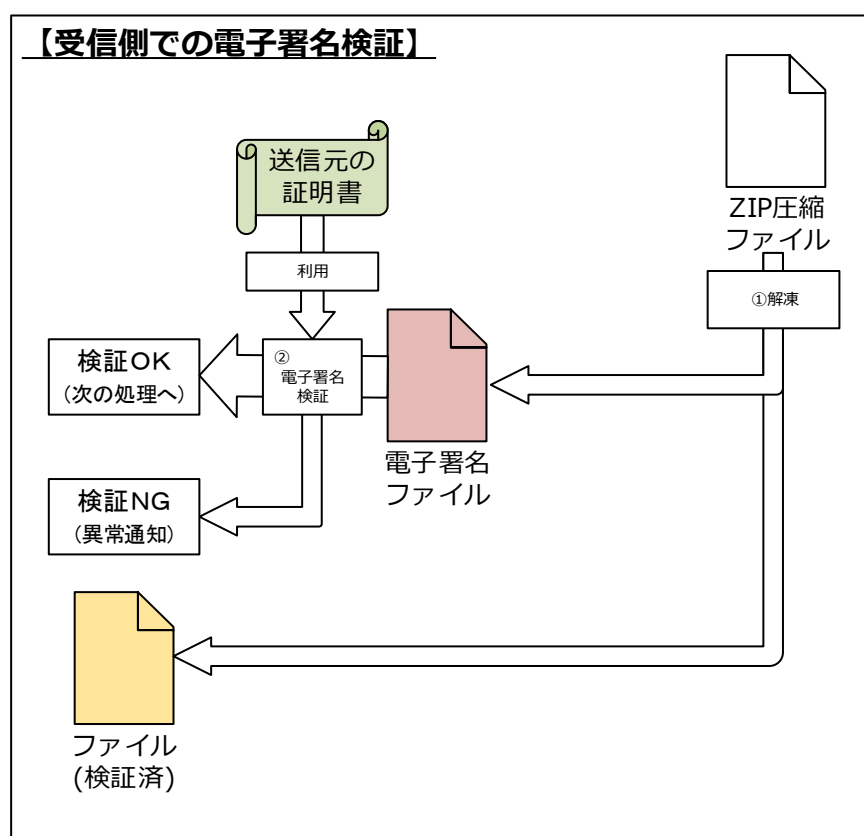


図 4-13:受信側での電子署名検証方式

- ① 「ZIP 圧縮ファイル」を解凍し、「電子署名ファイル」を抽出する。
- ② 「送信元の証明書」を利用して、①で抽出した「電子署名ファイル」を検証し、検証 OK であれば次の処理を実行する。（検証 NG の場合は、異常を通知する。）

(b) 電子署名アルゴリズム

電子署名付与/検証に利用する電子署名アルゴリズムを以下に示す(表 4-10)。

表 4-10: 電子署名アルゴリズム

No	区分	方式
1	署名	RSASSA-PKCS1-v1_5
2	メッセージダイジェスト	SHA-256
3	メッセージ認証コード	HMAC

4.1.4 データマスキング方式

(1) システムデータ

システムデータのマスキング方式は、以下に図示した手順で実施する。(図 4-14、図 4-15)

【送信側でのマスキング方式】

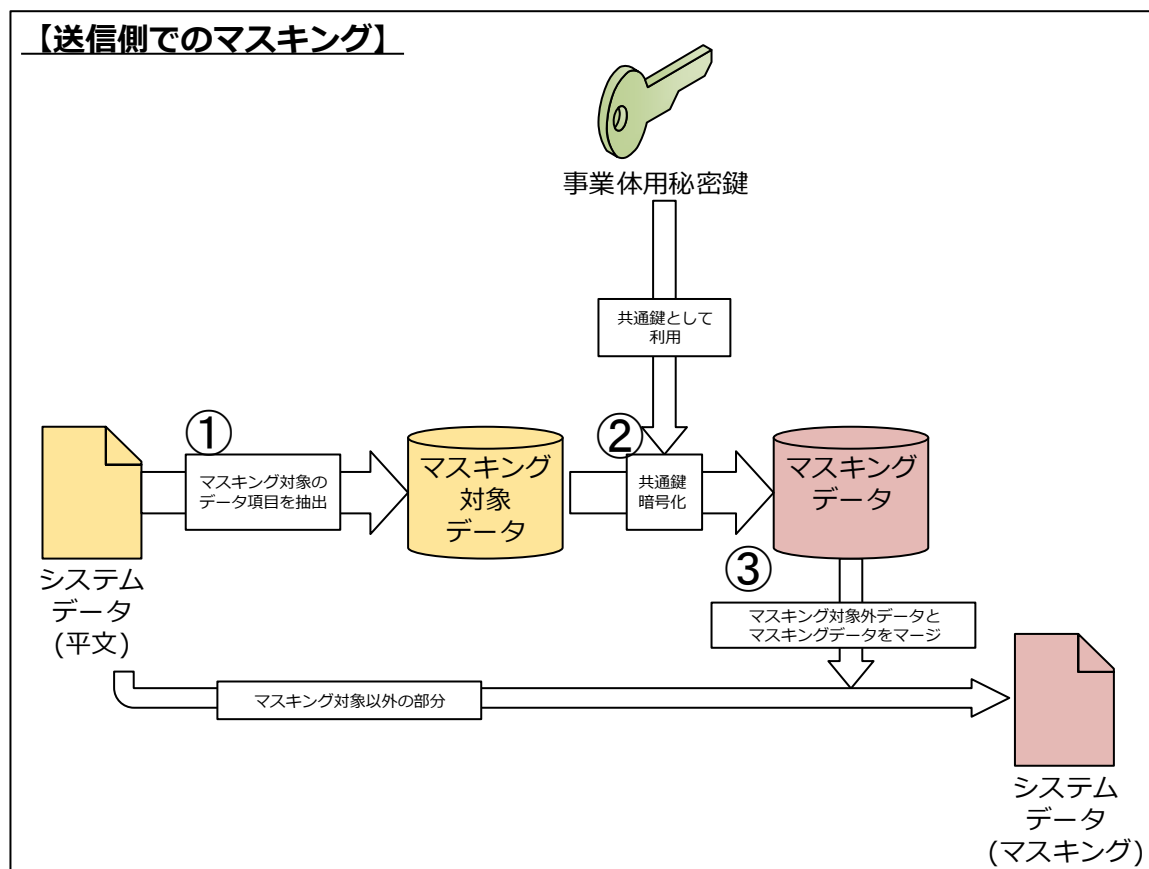


図 4-14: 送信側でのマスキング方式

- ① 「システムデータ (平文)」からマスキング対象データ項目を「マスキング対象データ」として抽出する。
- ② 事業体用の「秘密鍵」を共通鍵として、①で抽出した「マスキング対象データ」を共通鍵暗号方式で暗号化し、「マスキングデータ」を生成する。
- ③ マスキング対象以外のデータ項目と②で生成した「マスキングデータ」をマージして、「システムデータ (マスキング)」を生成する。

【受信側でのマスキング解除方式】

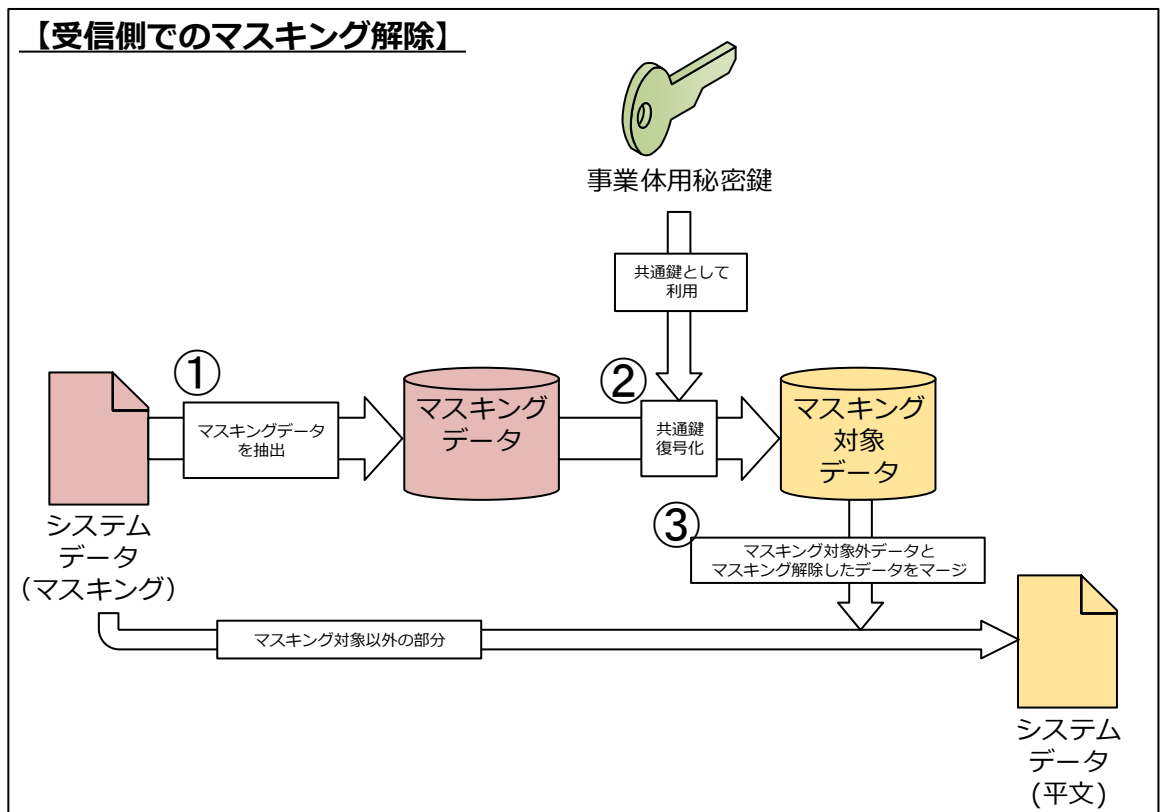


図 4-15:受信側でのマスキング解除方式

- ① 「システムデータ（マスキング）」からマスキング対象データを「マスキングデータ」として抽出する。
- ② 事業体の「秘密鍵」を共通鍵として、①で抽出した「マスキングデータ」を復号し、「マスキング対象データ」（マスキング解除データ）を生成する。
- ③ マスキング対象以外のデータ項目と②で生成した「マスキング対象データ」（マスキング解除データ）をマージして「システムデータ（平文）」を生成する。

4.2 機能要件

4.2.1 データ保護用証明書/秘密鍵取得機能

(1) 機能概要

機器ベンダー向け標準インターフェイス(デバイス)を通じて、水道標準プラットフォームからアプリケーション証明書(データ保護用)、水道標準プラットフォーム証明書(データ保護用)、ルート証明書、証明書失効リストを取得する処理を行う。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)にデータ保護用公開鍵証明書ファイル取得要求を送信する。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)からデータ保護用公開鍵証明書ファイルを受信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 4-16)。

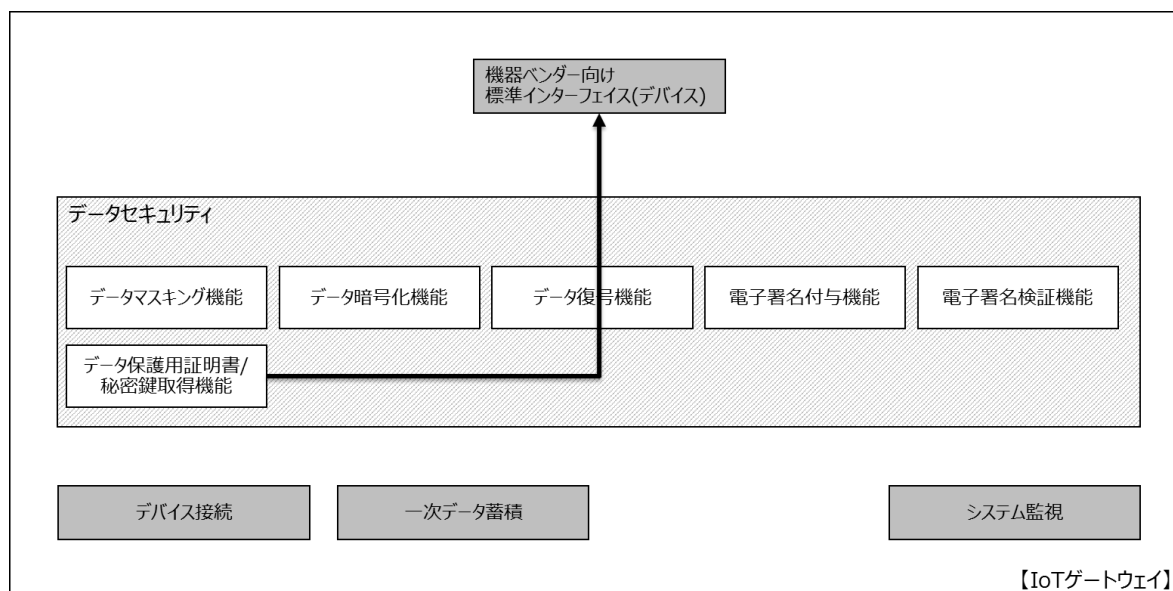


図 4-16: データ保護用証明書/秘密鍵取得機能 提供経路

4.2.2 データ暗号化機能

(1) 機能概要

社会インフラ水道情報活用システム標準仕様に準拠した通信データの暗号化を実施する処理を行う。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)からデータ暗号化対象のデータを受信する。
- ・ 機器ベンダー向け標準インターフェイス(デバイス)に暗号化済みデータを送信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 4-17)。

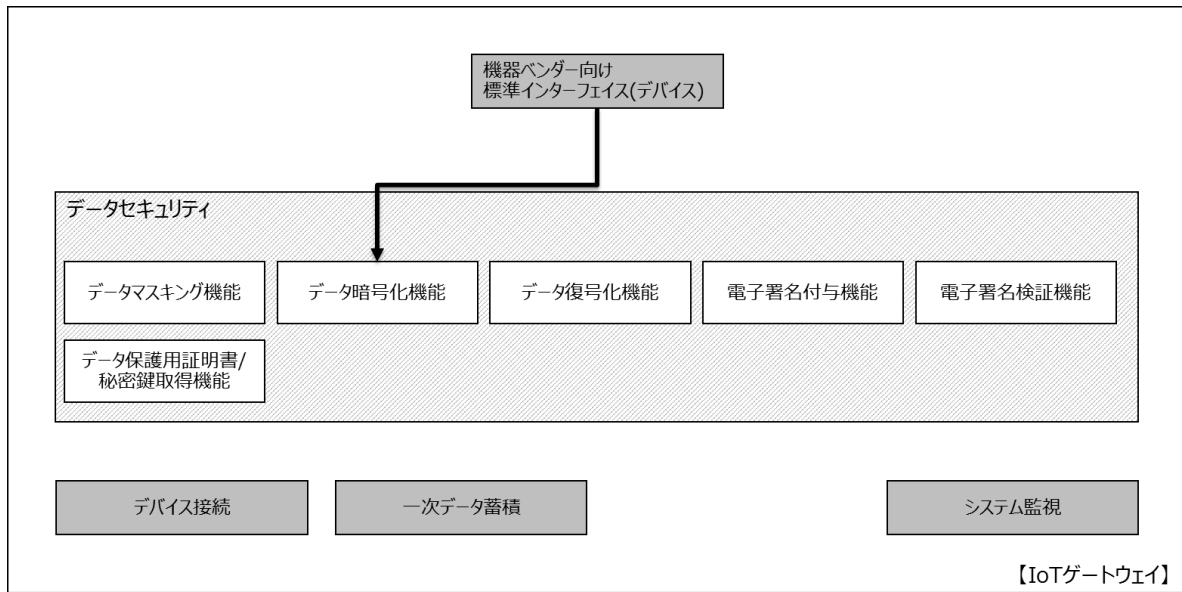


図 4-17: データ暗号化機能 提供経路

4.2.3 データ復号機能

(1) 機能概要

社会インフラ水道情報活用システム標準仕様に準拠した通信データの復号を実施する処理を行う。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)からデータ復号対象のデータを受信する。
- ・ 機器ベンダー向け標準インターフェイス(デバイス)に復号済みデータを送信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 4-18)。

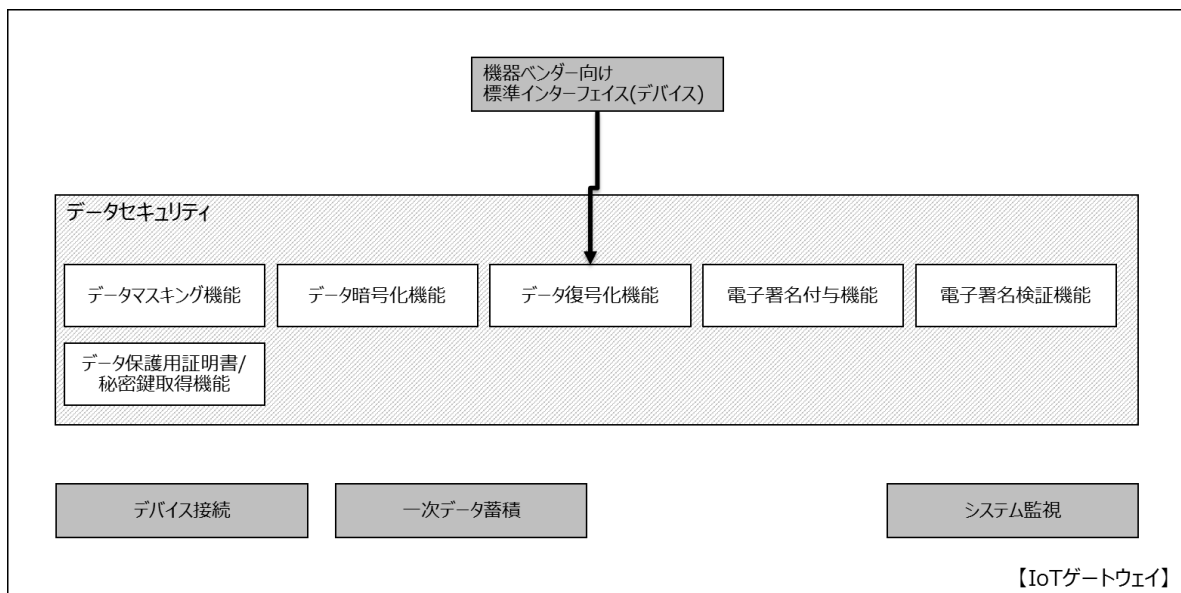


図 4-18: データ復号機能 提供経路

4.2.4 電子署名付与機能

(1) 機能概要

社会インフラ水道情報活用システム標準仕様に準拠した通信データの電子署名を付与する処理を行う。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)から電子署名付与対象のデータを受信する。
- ・ 機器ベンダー向け標準インターフェイス(デバイス)に電子署名済みデータを送信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 4-19)。

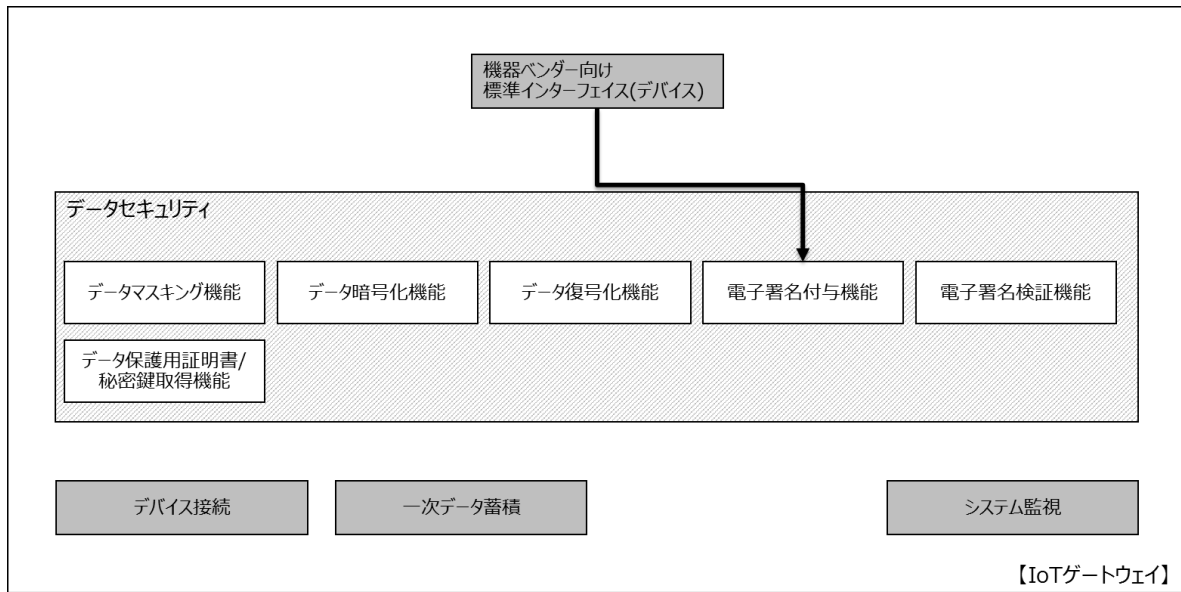


図 4-19: 電子署名付与機能 提供経路

4.2.5 電子署名検証機能

(1) 機能概要

社会インフラ水道情報活用システム標準仕様に準拠した通信データの電子署名を検証する処理を行う。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)から電子署名検証対象のデータを受信する。
- ・ 機器ベンダー向け標準インターフェイス(デバイス)に電子署名検証結果を送信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 4-20)。

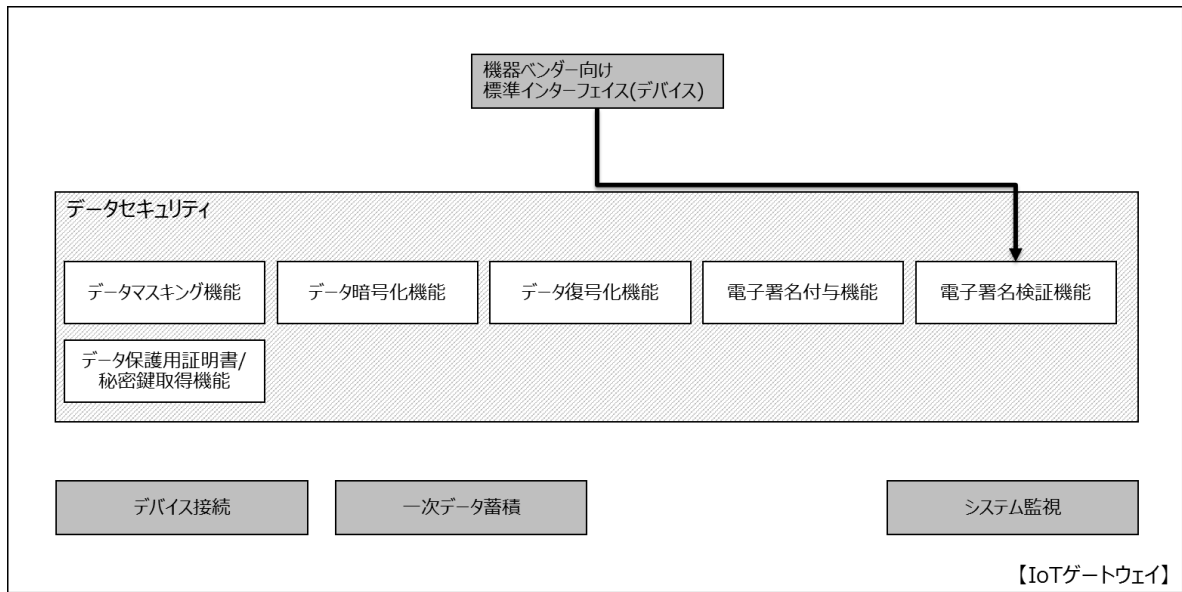


図 4-20: 電子署名検証機能 提供経路

4.2.6 データマスキング機能

(1) 機能概要

事業体用秘密鍵を用いて、既存システムの任意のデータ項目をマスキングする。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)からマスキング対象のデータを受信する。
- ・ 機器ベンダー向け標準インターフェイス(デバイス)にマスキング結果を送信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 4-21 図 4-20)。

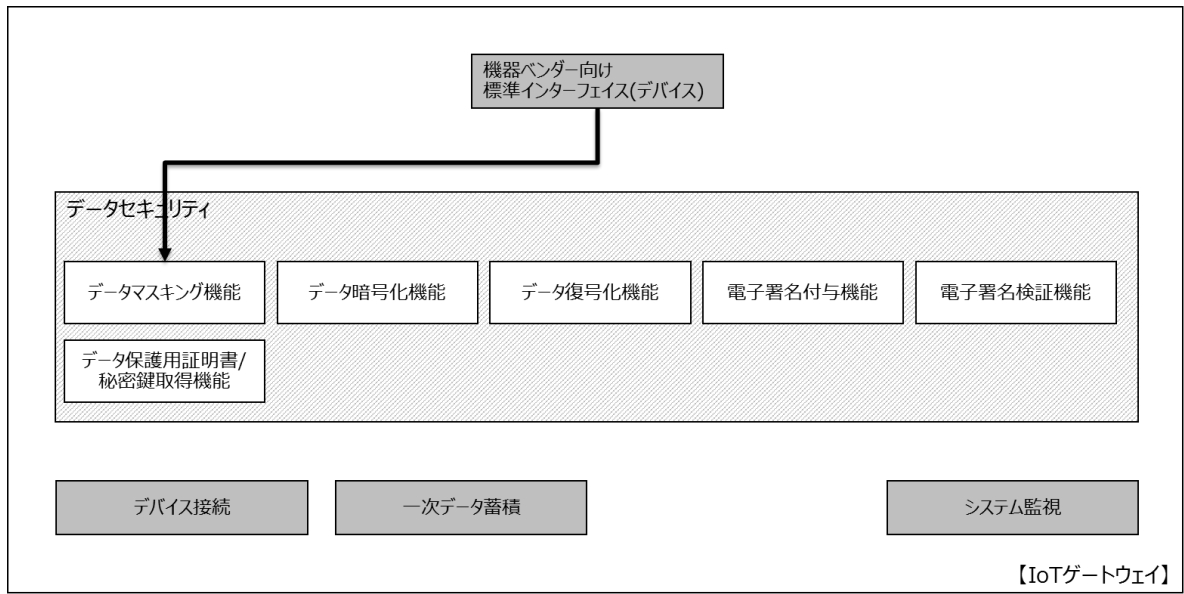


図 4-21: データマスキング機能 提供経路

5. 一次データ蓄積モジュール

5.1 機能概要

一次データ蓄積は、デバイスから取得したデータをゲートウェイ内に蓄積し、機器ベンダー向け標準インターフェイス(デバイス)の再送要求に応じてデータを提供する機能を提供する。

なお、本モジュールは、蓄積されたデータの改ざんや不正な読み取りを防止するため、耐タンパー性を高めておくことが望ましい。

5.2 機能一覧

本機能におけるモジュール機能の一覧をに示す(表 5-1、図 5-1)。

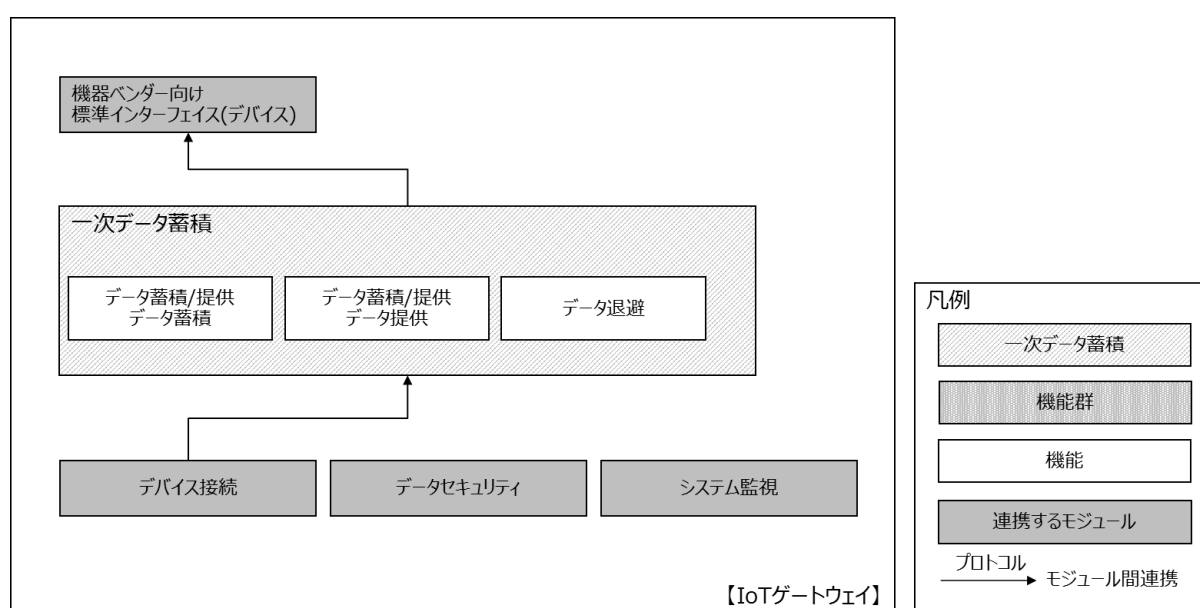


図 5-1: 一次データ蓄積機能(モジュール)構成

表 5-1: 一次データ蓄積 機能一覧

No	機能	概要説明
1	データ蓄積/提供	通信回線不調等による再送用にデータを一時的に蓄積する機能を提供する。
2	データ蓄積	デバイス接続/システム接続により取得したデータを蓄積する処理を提供する。
3	データ提供	機器ベンダー向け標準インターフェイス(デバイス)からの再送要求に従い、再送対象データを提供する。
4	データ退避	一定期間経過した蓄積データを外部ファイルに出力する処理を提供する。

5.3 機能要件

5.3.1 データ蓄積/提供-データ蓄積

(1) 機能概要

デバイス接続により取得したデータを蓄積する処理を提供する。

- ・ デバイス接続から一次データ蓄積のデータ蓄積実行要求を受信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 5-2)。

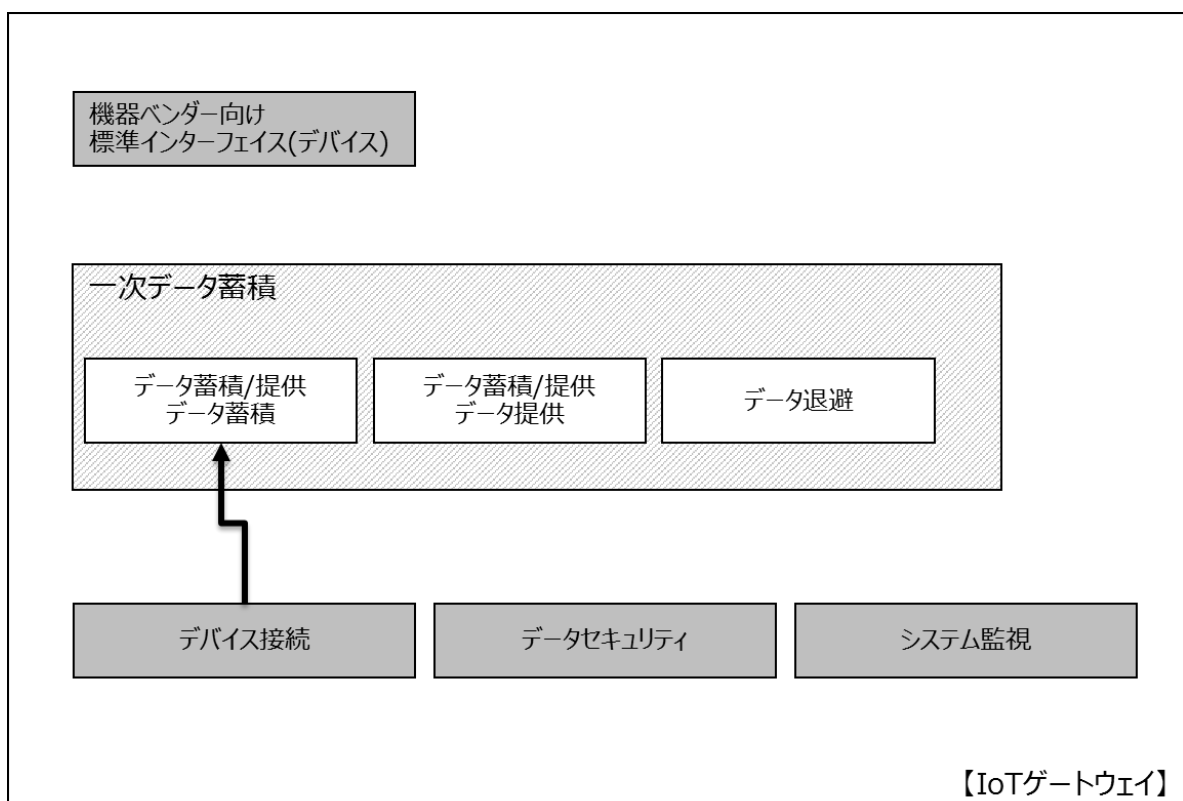


図 5-2: データ蓄積/提供-データ蓄積機能 提供経路

5.3.2 データ蓄積/提供-データ提供

(1) 機能概要

機器ベンダー向け標準インターフェイス(デバイス)からの再送要求に従い、再送対象データを提供する。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)から一次データ蓄積のデータ提供実行要求を受信する。

- ・ 一次データ蓄積から機器ベンダー向け標準インターフェイス(デバイス)にデータ提供実行結果を送信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 5-3)。

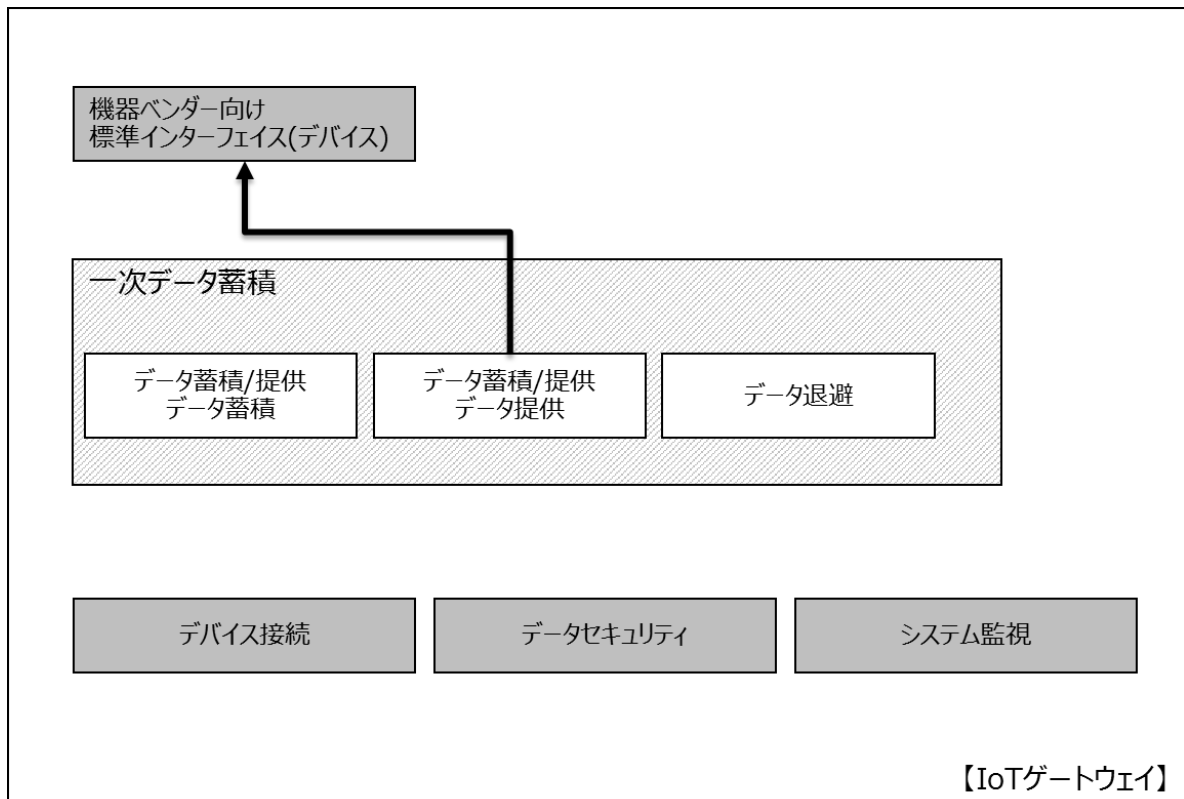


図 5-3: データ蓄積/提供-データ提供機能 提供経路

5.3.3 データ退避

(1) 機能概要

一定期間経過した蓄積データを外部ファイルに出力する処理を提供する。

- ・ 一次データ蓄積のデータ退避実行要求を受信し、データ退避を実行する。(機能内処理)

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 5-4)。

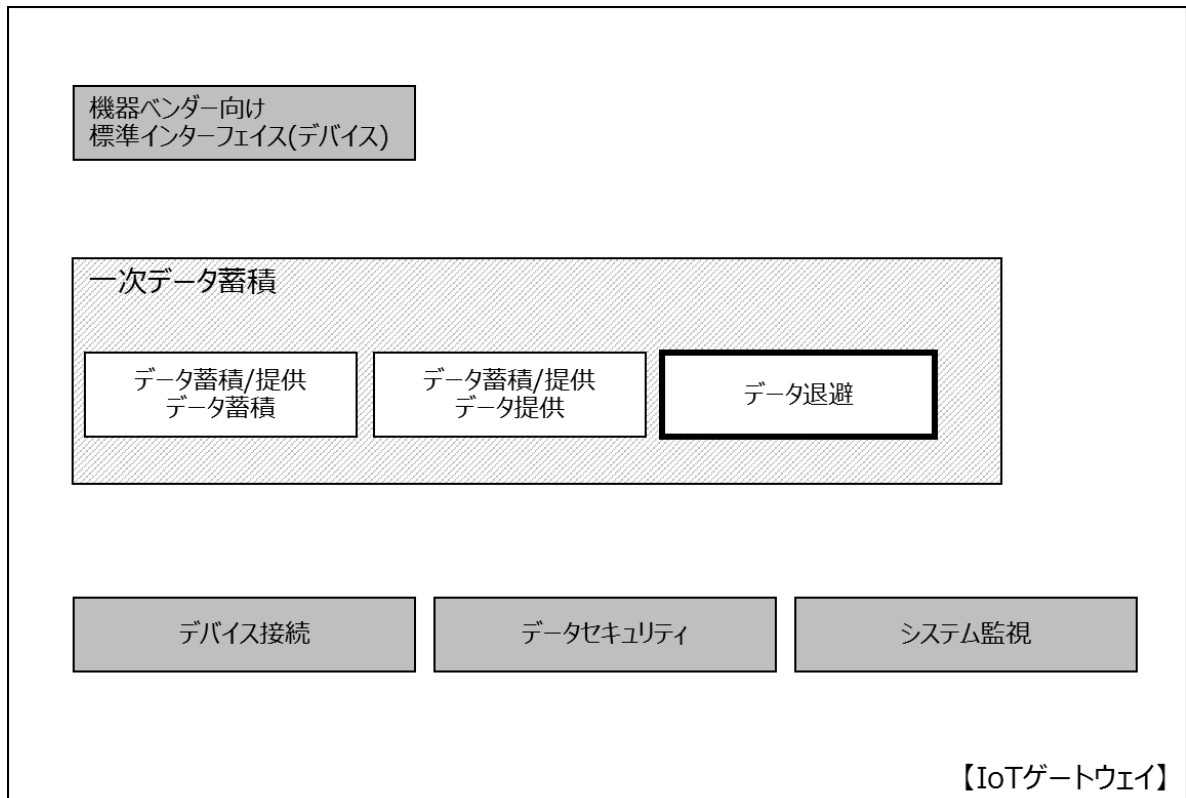


図 5-4: データ退避機能 提供経路

6. デバイス接続モジュール

6.1 機能概要

IoT ゲートウェイとデバイス間でデータをやり取りする機能を提供する。

6.2 機能一覧

本機能におけるモジュール機能の一覧をに示す(図 6-1、表 6-1)。

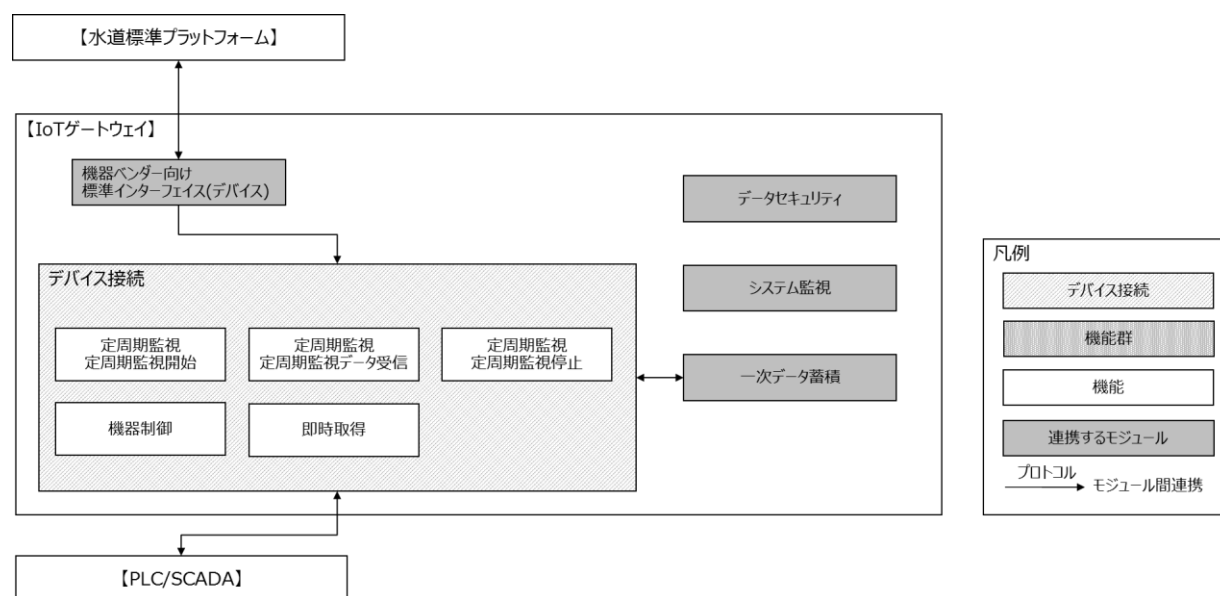


図 6-1: デバイス接続機能(モジュール)構成

表 6-1: デバイス接続 機能一覧

No	機能	概要説明
1	定周期監視	デバイスから定周期計測対象データを取得し、機器ベンダー向け標準インターフェイス(デバイス)へ連携する機能
2	定周期監視開始	機器ベンダー向け標準インターフェイス(デバイス)による要求に従って、定周期監視を開始する処理を実行する
3	定周期監視データ受信	デバイスから計測対象データを取得し、機器ベンダー向け標準インターフェイス(デバイス)へ連携する処理を実行する
4	定周期監視停止	機器ベンダー向け標準インターフェイス(デバイス)による要求に従って、定周期監視を停止する処理を実行する
5	即時取得	機器ベンダー向け標準インターフェイス(デバイス)による要求に従って、計測対象データを取得し、機器ベンダー向け標準インターフェイス(デバイス)へ連携する処理を実行する
6	機器制御	機器ベンダー向け標準インターフェイス(デバイス)による要求に従って、デバイスに制御操作を実行し、結果を機器ベ

		ンダー向け標準インターフェイス(デバイス)へ連携する処理を実行する
--	--	-----------------------------------

6.3 機能要件

6.3.1 定周期監視-定周期監視開始

(1) 機能概要

機器ベンダー向け標準インターフェイス(デバイス)による要求に従って、定周期監視を開始する処理を実行する。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)から定周期監視開始要求を受信する。
- ・ デバイス接続から機器ベンダー向け標準インターフェイス(デバイス)に定周期監視開始結果を送信する。
- ・ 機器ベンダー向け標準インターフェイス(デバイス)から定周期監視開始要求通信結果を受信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 6-2)。

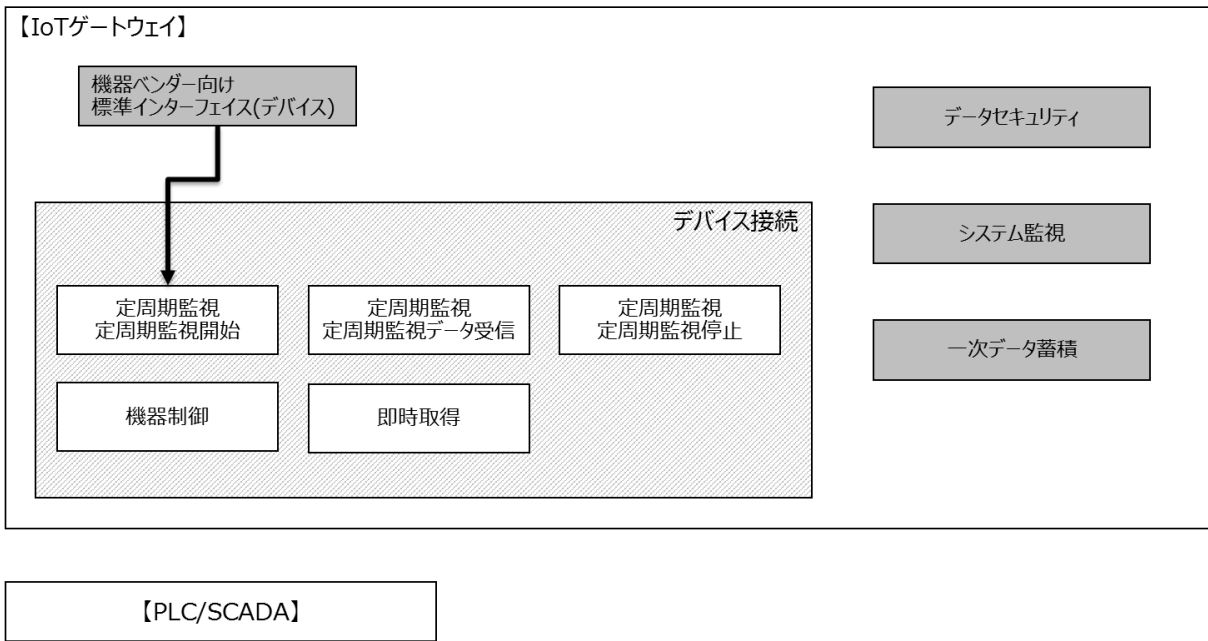


図 6-2: 定周期監視-定周期監視開始機能 提供経路

6.3.2 定周期監視-定周期監視データ受信

(1) 機能概要

デバイスから計測対象データを取得し、機器ベンダー向け標準インターフェイス(デバイス)へ連携する処理を実行する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 6-3)。

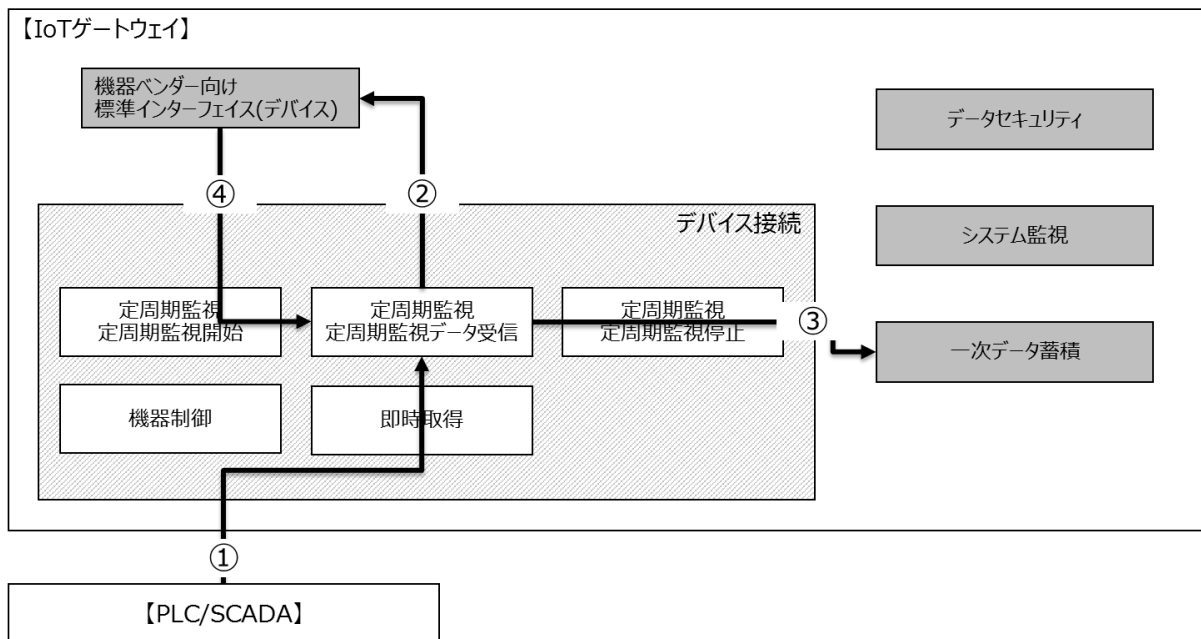


図 6-3: 定周期監視-定周期監視データ受信機能 提供経路

処理概要は以下の通り(表 6-2)。

表 6-2: 定周期監視-定周期監視データ受信機能 処理概要

No	処理概要
1	PLC から定周期監視データを受信する。
2	デバイス接続から機器ベンダー向け標準インターフェイス(デバイス)に定周期監視データ送信要求を送信する。
3	デバイス接続から一次データ蓄積に定周期監視データ蓄積機能実行を要求する。一次データ蓄積から定周期監視データ蓄積機能実行結果を受信する。
4	機器ベンダー向け標準インターフェイス(デバイス)から定周期監視データ送信要求通信結果を受信する。

6.3.3 定周期監視-定周期監視停止

(1) 機能概要

機器ベンダー向け標準インターフェイス(デバイス)による要求に従って、定周期監視を停止する処理を実行する。

- ・ 機器ベンダー向け標準インターフェイス(デバイス)から定周期監視停止要求を受信する。
- ・ デバイス接続から機器ベンダー向け標準インターフェイス(デバイス)に定周期監視停止結果を送信する。
- ・ 機器ベンダー向け標準インターフェイス(デバイス)から定周期監視停止要求通信結果を受信する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 6-4)。

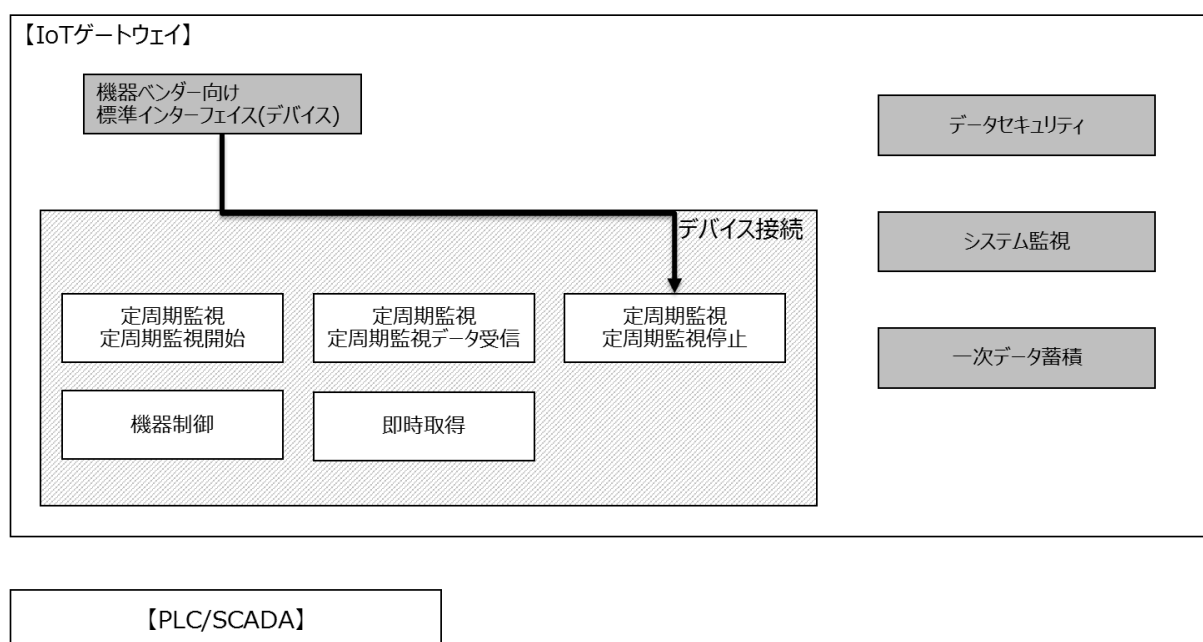


図 6-4: 定周期監視-定周期監視停止機能 提供経路

6.3.4 即時取得

(1) 機能概要

機器ベンダー向け標準インターフェイス(デバイス)による要求に従って、計測対象データを取得し、機器ベンダー向け標準インターフェイス(デバイス)へ連携する処理を実行する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 6-5)。

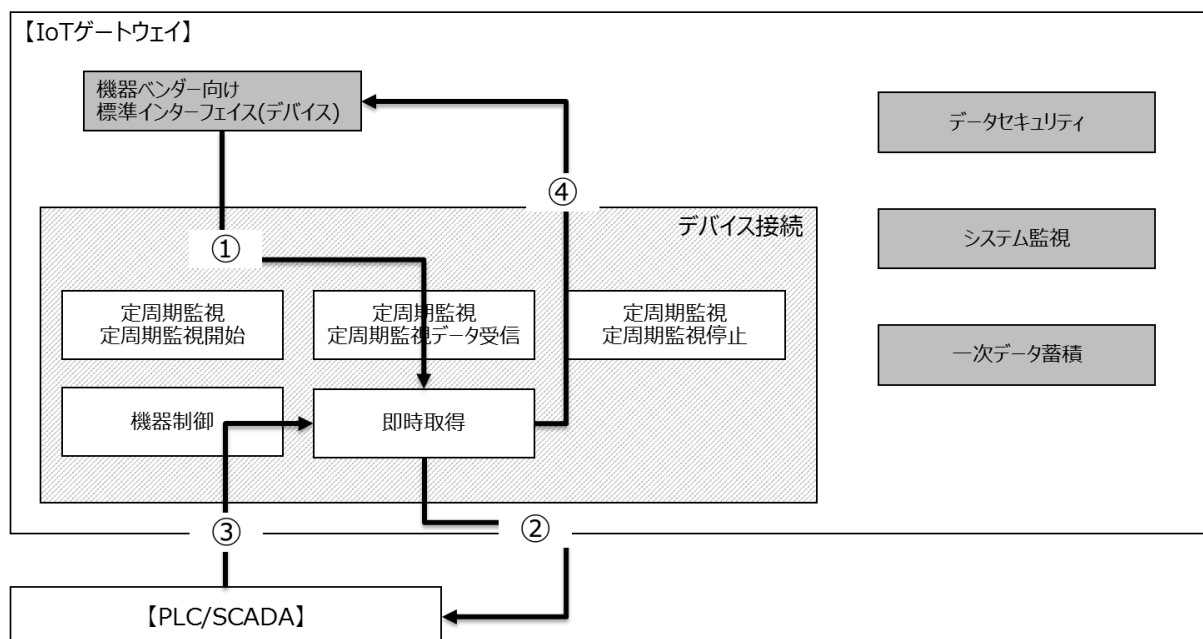


図 6-5: 即時取得機能 提供経路

処理概要は以下の通り(表 6-3)。

表 6-3: 即時取得機能 処理概要

No	処理概要
1	機器ベンダー向け標準インターフェイス(デバイス)から即時取得要求を受信する。
2	デバイス接続から PLC にデータ取得要求を送信する。
3	PCL から要求データを受信する。
4	デバイス接続から機器ベンダー向け標準インターフェイス(デバイス)に即時取得結果を送信する。

6.3.5 機器制御

(1) 機能概要

機器ベンダー向け標準インターフェイス(デバイス)による要求に従って、デバイスに制御操作を実行し、結果を機器ベンダー向け標準インターフェイス(デバイス)へ連携する処理を実行する。

(2) 提供経路

機能を提供経路する経路を以下に図示する(図 6-6)。

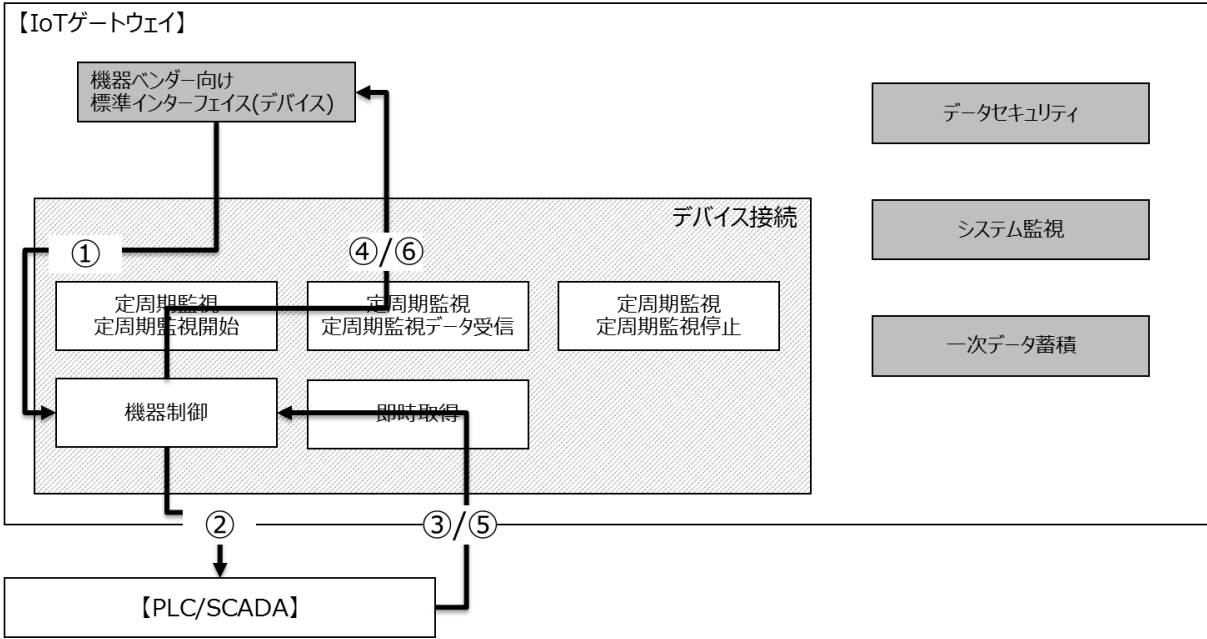


図 6-6: 制御操作機能 提供経路

処理概要は以下の通り(表 6-4)。

表 6-4: 機器制御機能 処理概要

No	処理概要
1	機器ベンダー向け標準インターフェイス(デバイス)から制御操作要求を受信する。
2	デバイス接続から PLC に制御操作要求を送信する。
3	PLC から制御操作要求完了通知を受信する。

No	処理概要
4	デバイス接続から機器ベンダー向け標準インターフェイス(デバイス)に制御操作要求完了通知を送信する。
5	PLC から制御操作完了通知を受信する。
6	デバイス接続から機器ベンダー向け標準インターフェイス(デバイス)に制御操作完了通知を送信する。

7. システム監視モジュール

7.1 機能概要

システム監視は、水道標準プラットフォームのシステム管理者に対して、水道標準プラットフォームおよびゲートウェイのシステム状態を監視するための機能を提供する機能群である。水道標準プラットフォームのシステム管理者は、水道標準プラットフォームおよびゲートウェイのシステム状態を監視し、環境の故障を適切に検出することで可用性の確保を行う。また、水道情報活用システムを利用する事業者の事業者運用管理者に対しても、監視項目をリアルタイムで確認するための画面を提供することで、システム状態の共有を可能とする。

システム監視モジュールにより収集した IoT ゲートウェイのシステム監視情報は、水道標準プラットフォームに送信し、一元管理できるようにする。詳細は、“水道標準プラットフォーム外部仕様書”を参照すること。

- 以上 -